



Scan the code above or visit
www.nwleics.gov.uk/meetings for a full copy of the
agenda.

Meeting	AUDIT AND GOVERNANCE COMMITTEE
Time/Day/Date	6.30 pm on Wednesday, 26 July 2023
Location	Abbey Room, Stenson House, London Road, Coalville, LE67 3FN
Officer to contact	Democratic Services (01530 454512)

AGENDA

Item	Pages
1. APOLOGIES FOR ABSENCE	
2. DECLARATION OF INTERESTS	
Under the Code of Conduct members are reminded that in declaring interests you should make clear the nature of that interest and whether it is a disclosable pecuniary interest, registerable interest or other interest.	
3. MINUTES	
To confirm and sign the minutes of the meeting held on 26 April 2023	3 - 6
4. COMMITTEE WORK PLAN	
To note the Committee's work plan	7 - 10
5. CORPORATE RISK UPDATE	
Report of the Strategic Director	11 - 22
6. TREASURY MANAGEMENT ACTIVITY REPORT 2023/24 - QUARTER 1	
Report of the Head of Finance	23 - 40
7. REVIEW OF CORPORATE GOVERNANCE POLICIES	
Report of the Head of Finance	41 - 206
8. UPDATE ON THE CIPFA POSITION STATEMENT AND WORKING GROUP	
Report of the Audit Manager	207 - 220

9. INTERNAL AUDIT PROGRESS REPORT	
Report of the Audit Manager	221 - 244
10. INTERNAL AUDIT ANNUAL REPORT	
Report of the Audit Manager	245 - 256
11. MANAGEMENT RESPONSE AND ACTION PLAN TO ANNUAL INTERNAL AUDIT OPINION	
Report of the Strategic Director	257 - 266
12. STANDARDS AND ETHICS REPORT - QUARTER 1	
Report of the Monitoring Officer	267 - 278

Circulation:

Councillor D Everitt (Chair)
Councillor P Moulton (Deputy Chair)
Councillor R Boam
Councillor D Cooper
Councillor G Rogers
Councillor J G Simmons
Councillor N Smith
Councillor R Sutton
Councillor A Barker

MINUTES of a meeting of the AUDIT AND GOVERNANCE COMMITTEE held in the Boardroom, Council Offices, Coalville on WEDNESDAY, 26 APRIL 2023

Present: Councillor S Gillard (Chair)

Councillors E G C Allman, C C Benfield, J Clarke, R L Morris, V Richichi, S Sheahan and M B Wyatt

Officers: Mr G Hammons, Ms K Beavis, Mrs A Crouch, Mrs R Wallace and Miss E Warhurst

External Audit: Mrs L Parsons and Mr M SurrIDGE

85. APOLOGIES FOR ABSENCE

Apologies were received from Councillors M Haye and N Smith.

86. DECLARATION OF INTERESTS

There were no declarations of interest.

87. MINUTES

Consideration was given to the minutes of the meeting held on 15 March 2023.

It was moved by Councillor S Gillard, seconded by Councillor J Clarke and

RESOLVED THAT:

The minutes of the meeting held on 15 March 2023 be approved and signed by the Chair as a correct record.

88. AUDIT COMPLETION REPORT - FOLLOW UP LETTER

The Finance Team Manager introduced the item and handed over to the External Auditor to present the report to Members.

No comments were made.

It was moved by Councillor S Gillard, seconded by Councillor E Allman and

RESOLVED THAT:

The report be noted.

89. ANNUAL AUDITORS REPORT 2020/21

The Interim Head of Finance introduced the item and highlighted the updated appendix as detailed within the additional papers. The External Auditors then presented the report to Members.

A discussion was had on the pension and liability risk and the ability to mitigate this risk. The External Auditor confirmed that when the valuation was received at the end of May, it was likely that the liability position was almost gone, this could change in 2024 but the main concern was that the figures were correct, and they were.

At the request of a Member, further information was given in relation to the External Auditors additional fees. The Interim Head of Finance also explained that the Council was

receiving support from the Government in relation to the fees that were incurred due to the change in auditing standards.

In response to a question about any concerns with the Journey to Self-Sufficiency Fund, it was the External Auditor's opinion that the Council had delivered on budgets and financial stability and therefore was in a good position.

It was moved by Councillor S Gillard, seconded by Councillor R Morris and

RESOLVED THAT:

The report be noted.

90. EXTERNAL AUDIT STRATEGY MEMORANDUM 2021-22

The Interim Head of Finance introduced the item and handed over to External Audit to present the report to Members.

In response to a question, the External Auditor explained that the forthcoming district election was not included as a risk as this report was in relation to the year 2021/22.

It was moved by Councillor S Gillard, seconded by Councillor J Clarke and

RESOLVED THAT:

The report be noted.

91. ACCOUNTING POLICIES AND MATERIALITY 2022/23

The Finance Team Manager presented the report to Members.

No comments were made.

It was moved by Councillor S Gillard, seconded by Councillor E Allman and

RESOLVED THAT:

The Draft Accounting Policies for the 2022/23 Financial Statements as detailed in appendix A be approved.

92. TREASURY MANAGEMENT STEWARDSHIP REPORT 2022/23

The Finance Team Manager presented the report to Members.

No comments were made.

It was moved by Councillor S Gillard, seconded by Councillor E Allman and

RESOLVED THAT:

The report be approved.

93. INTERNAL AUDIT PROGRESS REPORT

The Audit Manager presented the report to Members.

No comments were made.

It was moved by Councillor S Gillard, seconded by Councillor R Morris and

RESOLVED THAT:

The report be noted.

94. CIPFA POSITION STATEMENT

The Audit Manager presented the report to Members.

No comments were made.

It was moved by Councillor S Gillard, seconded by Councillor E Allman and

RESOLVED THAT:

- 1) The report be noted.
- 2) A cross party member working group be established, to be drawn from the Audit and Governance Committee appointed at Council on 23 May 2023, to work with the Audit Manager and the Head of Legal and Support Services to undertake a self-assessment and training needs analysis and report back to the meeting of Audit and Governance Committee at the July meeting.
- 3) The process for the recruitment of independent members to the committee be agreed.

95. ANNUAL AUDIT PLAN

The Audit Manager presented the report to Members.

No comments were made.

It was moved by Councillor S Gillard, seconded by Councillor R Morris and

RESOLVED THAT:

- 1) The report be noted.
- 2) The 2023/24 Internal Audit Annual Plan be approved.

96. CORPORATE RISK UPDATE

The Interim Head of Finance presented the report to Members.

In response to a question in relation to cost of living and inflation, the Interim Head of Finance explained that this was still considered a risk and was being managed within other corporate risks.

During discussions on the management of the risk register, it was confirmed that previous registers were reviewed and used as a learning tool. Also, external assessments were undertaken to ascertain if any improvements could be made, there would be more information in relation to this in a future report.

In relation to a query about staff salaries and the risk of possible staff movement to the private sector due to salaries not being increased in line with inflation, the Interim Head of Finance confirmed the matter was being actively managed and regularly discussed.

It was moved by Councillor S Gillard, seconded by Councillor E Allman and

RESOLVED THAT:

The report be noted.

97. DRAFT MEMBER CONDUCT ANNUAL REPORT

The Head of Legal and Support Services presented the report to Members.

No comments were made.

It was moved by Councillor S Gillard, seconded by Councillor J Clarke and

RESOLVED THAT:

- 1) The Draft Member Conduct Annual Report 2022/23 be received and noted.
- 2) That authority be delegated to the Head of Legal and Support Services to make any minor amendments to the report following comments from the Audit and Governance Committee.

RECOMMENDED THAT:

Council endorses the Member Conduct Annual Report 2022/23.

98. STANDARDS AND ETHICS REPORT - QUARTER 4

The Head of Legal and Support Services presented the report to Members.

No comments were made.

It was moved by Councillor S Gillard, seconded by Councillor V Richichi and

RESOLVED THAT:

The report be received and noted.

The meeting commenced at 6.30 pm

The Chairman closed the meeting at 7.10 pm

AUDIT AND GOVERNANCE COMMITTEE – WORK PROGRAMME (as at 18/07/23)

Issue	Report Author	Meeting at which will be reported
27 September 2023		
Annual Governance Statement 2021/22 and 2022/23	Glenn Hammons, Strategic Director of Resources (Section 151 Officer)	27 September 2023
Annual Completion Report 2021/22	Glenn Hammons, Strategic Director of Resources (Section 151 Officer)	27 September 2023
Annual Statement of Accounts 2021/22 For the Audit and Governance Committee to consider and approve the Statement of Accounts 2021/22.	Anna Crouch, Head of Finance	27 September 2023
Local Government and Social Care Ombudsman Review Letter 2022/23	Elizabeth Warhurst, Head of Legal and Support Services (Monitoring Officer)	27 September 2023
25 October 2023		
Annual Auditors Report 2021/22 To consider the External Auditors Report	Anna Crouch, Head of Finance	25 October 2023
External Audit Strategy Memorandum 2022-23 To consider the External Auditors Report	Anna Crouch, Head of Finance	25 October 2023
Treasury Management Activity Report 2023/24 - Quarter 2 To inform Members of the Treasury Activity for the period.	Anna Crouch, Head of Finance	25 October 2023
Update on Action Plan in Response to Annual Internal Audit Opinion 2022/23	Glenn Hammons, Strategic Director of Resources (Section 151 Officer)	25 October 2023
Internal Audit Progress Report	Kerry Beavis, Audit Manager	25 October 2023
Standards and Ethics Report - Quarter 2	Rebecca Elliott, Solicitor - Contracts and Commercial	25 October 2023

7

Issue	Report Author	Meeting at which will be reported
Corporate Risk Update	Glenn Hammons, Strategic Director of Resources (Section 151 Officer)	25 October 2023
Update on the CIPFA Position Statement and Working Group	Kerry Beavis, Audit Manager	25 October 2023
24 January 2024		
Annual Review of the Council's Constitution	Kate Hiller, Legal Team Manager and Deputy Monitoring Officer	24 January 2024
Treasury Management Activity Report 2023/24 - Quarter 3 To inform Members of the Treasury Activity for the period.	Anna Crouch, Head of Finance	24 January 2024
Internal Audit Progress Report	Kerry Beavis, Audit Manager	24 January 2024
Standards and Ethics Report - Quarter 3	Rebecca Elliott, Solicitor - Contracts and Commercial	24 January 2024
Corporate Risk Update	Glenn Hammons, Strategic Director of Resources (Section 151 Officer)	24 January 2024
Update on the CIPFA Position Statement and Working Group	Kerry Beavis, Audit Manager	24 January 2024
Update on Action Plan in Response to Annual Internal Audit Opinion 2022/23	Glenn Hammons, Strategic Director of Resources (Section 151 Officer)	24 January 2024
13 March 2024		
2022/23 Audit Completion Report To consider the External Auditors Report	Anna Crouch, Head of Finance	13 March 2024
Annual Statement of Accounts 2022/23 For the Audit and Governance Committee to consider and approve the Statement of Accounts 2022/23.	Anna Crouch, Head of Finance	13 March 2024
24 April 2024		

Issue	Report Author	Meeting at which will be reported
2022/23 Annual Auditors Report To consider the External Auditors Report	Anna Crouch, Head of Finance	24 April 2024
External Audit Strategy Memorandum 2023-24 To consider the External Auditors Report.	Anna Crouch, Head of Finance	24 April 2024
Draft Accounting Policies 2023/24 To present the draft accounting policies for the 2023/24 financial statements	Anna Crouch, Head of Finance	24 April 2024
Draft Treasury Management Stewardship Report 2023/24 For the Audit and Governance Committee to consider the draft Treasury Management Stewardship Report 2023/24 before it is presented to Cabinet.	Anna Crouch, Head of Finance	24 April 2024
Draft Member Code of Conduct Annual Report	Rebecca Elliott, Solicitor - Contracts and Commercial	24 April 2024
Internal Audit Progress Report	Kerry Beavis, Audit Manager	24 April 2024
Standards and Ethics Report - Quarter 4	Rebecca Elliott, Solicitor - Contracts and Commercial	24 April 2024
Corporate Risk Update	Glenn Hammons, Strategic Director of Resources (Section 151 Officer)	24 April 2024
Update on the CIPFA Position Statement and Working Group	Kerry Beavis, Audit Manager	24 April 2024
Update on Action Plan in Response to Annual Internal Audit Opinion 2022/23	Glenn Hammons, Strategic Director of Resources (Section 151 Officer)	24 April 2024

This page is intentionally left blank

NORTH WEST LEICESTERSHIRE DISTRICT COUNCIL

AUDIT AND GOVERNANCE COMMITTEE – WEDNESDAY,
26 JULY 2023



Title of Report	CORPORATE RISK UPDATE	
Presented by	Glenn Hammons Interim Director for Resources	
Background Papers	Corporate Risk Update (Audit and Governance Committee – April 2023) NORTH WEST LEICESTERSHIRE DISTRICT COUNCIL (nwleics.gov.uk)	Public Report: Yes
Purpose of Report	To provide Committee members with an update in respect of the Council's corporate risk register.	
Recommendations	THAT THE AUDIT AND GOVERNANCE COMMITTEE NOTES AND COMMENTS ON THE LATEST CORPORATE RISK REGISTER FOR CONSIDERATION BY THE RISK SCRUTINY GROUP.	

1.0 BACKGROUND

- 1.1 As part of the agreed Risk Management approach this report presents the latest version of the Corporate Risk Register as reviewed at the last meeting of the Risk Scrutiny Group on 29 June 2023. In line with the policy, members of this Committee, and Cabinet are to receive periodic updates on risks monitored through the Corporate Risk Register.
- 1.2 The updated Risk Register can be found at Appendix 1 and a summary of changes since the last update in April 2023 is set out below.
- 1.3 Out of the 17 active risks, 0 are Red, 7 are Amber and 10 are Green. Two new potential risks have been identified as Risks 15 and 16 in Appendix 1. A summary of these are set out in the table below. As these are new risks they will be monitored over the next cycle and more fully reported to the committee should it develop further.

Risk Ref	Risk Title	Summary of Risk
15	ORGANISATIONAL//POLITICAL No Overall Control of Council following the May 2023 Elections	No overall control of the Council following the May 2023 elections could lead to instability in the decision making process which could impact adversely on service delivery
16	ORGANISATIONAL/REPUTATIONAL Adverse External Assessment	There is greater focus from Government and regulators on the local government sector. There is a risk of an impact of an adverse external assessment on the Council. If this risk materialised it could impact on service delivery, performance levels, governance and decision making arrangements

- 1.4 The Director of Resources acts as lead for corporate risk and is satisfied that the main risks posed to the organisation have been captured within the risk register and that control measures to mitigate these risks are appropriate. The report is based on an update in July 2023, any further update on significant changes in risk will be provided at the meeting.
- 1.5 To ensure the Council's risk management approach is working effectively an external review was undertaken by Zurich (the Council's insurers). The review took place in 2022/23. The draft report received by the Council acknowledged a number of positive actions the Council is taking in its risk management approach, it also identified a few areas for improvement. The Council is currently working with Zurich to develop an Action Plan in response to the recommendations. This will be presented to the Committee at its next meeting. Overall the Council's risk management approach is in line with other local authorities.
- 1.6 The Risk Management Strategy and Framework is reviewed and refreshed on an annual basis. The updated Strategy for 2023 is included as part of the Review of Corporate Policies report included elsewhere on the Committees agenda. This primary update to the Strategy is to include a section on the current challenges/environment within which the council is operating. The inclusion of this in the Strategy follows a recommendation from an external review of the Council's approach to risk.
- 1.7 The Audit and Governance Committee are asked to review and note this risk update, and provide any feedback they wish to be considered by the Risk Scrutiny Group at its next meeting.

Policies and other considerations, as appropriate	
Council Priorities:	Effective risk management underpins the ability of the Council to deliver against all its priorities.
Policy Considerations:	None
Safeguarding:	None
Equalities/Diversity:	None
Customer Impact:	None
Economic and Social Impact:	None
Environment and Climate Change:	None
Consultation/Community Engagement:	None
Risks:	The Council manages its risks within existing budgets. Effective risk management protects the Council from insurance and/or compensation claims, fraud, and a range of other financial and non financial risks
Officer Contact	Glenn Hammons Director for Resources Glenn.hammons@nwleicestershire.gov.uk

This page is intentionally left blank

Corporate Risk Register													
Ref No.	Risk Description	Consequence	Cause	Inherent Risk			Responsibility of	Responsible to	Control Measures	Residual Risk			Movement of Risk
				Impact	Likelihood	Rating				Impact	Likelihood	Rating	
1	SOCIAL/ POLITICAL/ LEGAL Death / serious harm to a vulnerable person receiving a council service and safeguarding compliance	A serious case review arising from death/serious harm to a vulnerable person. Reputational damage to council. Loss of confidence in ability of council to deliver services. Ensuring compliance with Safeguarding legislation and practise.	Lack of response to a safeguarding report.	3	3	9	Environmental Health and Community Safety Team Manager	Head of Community Services	The organisation has the following structures in place;	3	1	3	Stable
			Service failure.						A recent audit with action plan of reasonable assurance				
			Modern slavery.						An identified Corporate Lead				
			poor safeguarding assurance						An identified Team responsible for Safeguarding (Community Safety) with responsibility embedded into Team Leader role and an officer (Child & Adults at risk Officer)				
									An agreed Safeguarding Policy refreshed as required				
									An identified group of Designated Safeguarding Officers (DSO's)				
									A programme of regular DSO meetings which consider training, best practice and case issues				
									An annual training programme to ensure new DSO's are well informed and trained				
									A quarterly senior management review by the Head of Community Services of all cases to check progress/close cases				
									Annual report to CLT and Corporate Scrutiny as required by exception.				
									Commitment to raise awareness of the scale and extent of modern slavery in the UK and ensure our contracts and supplies don't contribute to modern day slavery and exploitation.				
									A computerised system of reporting and managing reports introduced in 2019, will ensure constant reminders of new cases, sending alerts at all points in the procedure.				
			2						FINANCIAL/ COMMERCIAL/ REPUTATIONAL Mismanagement of council finances				
Poor budget planning / management.	Regular management reviews monitor actual spend against budgets and forecast to the end of the year.												
Internal financial systems and regulations not being properly applied.	Regular reporting and challenging at CLT, and reported to Cabinet quarterly Sound policies and procedures are in place.												
	Financial planning processes have been documented and are reviewed regularly.												
	Internal and External audit of systems and accounts.												
	Procurement of new finance system with increased controls and monitoring underway												
3	REPUTAITONAL/ COMMERCIAL Insufficient resources due to unplanned / unforeseen absences / vacancies / changes to financial picture	Council unable to perform its statutory duties and/or deliver objectives. Council's Partners unable to perform duties. Inflationary pressures. Use of external resources at significantly higher cost. Short / Medium Term Exposure.	Failure to horizon scan and interpret future needs in crucial roles.	3	3	9	Head of HR and OD & Head of Finance Ds151	Chief Executive	Membership of CIPFA and engagement of Arling Close gives access to specialist advice, analysis and expertise.	3	2	6	Stable
			Changes to income or financial climate						Current and forecasted balance MTFs, although uncertainty regarding future gov funding streams and impacts of changes such as DevCo/Freeport etc				

Corporate Risk Register													
Ref No.	Risk Description	Consequence	Cause	Inherent Risk			Responsibility of	Responsible to	Control Measures	Residual Risk			Movement of Risk
				Impact	Likelihood	Rating				Impact	Likelihood	Rating	
			Inability to recruit to vacancies / retain staff globally or in specialist areas .						Advance planning to mitigate this risk; recent COVID experience demonstrates NWL able to react and adjust				
									Recruitment and retention report considered by CLT and non pay benefits improved during the last year to attract and develop the right skills, and promoting existing staff talent through secondments and tailored development programmes. IIP. silver award achieved in 2022. New focus on Apprenticeships development to allow the Council to 'grow our own' and to tackle ageing workforce distribution.				
			unexpected or unplanned event (eg pandemic)						Ability to divert resources from other services, bringing in additional resources from other sources (e.g. Agencies, Consultants, Voluntary/ Community sector etc.) would be activated.				
									Market conditions are tested through recruitment processes, some challenges in some specialist areas				
									The Council can offer a package of additional benefits to enhance the recruitment offer.				
									Mitigations in place for variety of staffing related aspects - eg mental health awareness, overall wellbeing work etc				
									The Council has developed innovative partnering relationships with other sectors including the private sector to make posts uniquely attractive.				
5	4 LEGAL / FINANCIAL Contracts are not properly procured and managed	Council liable to incur additional costs, contract overrun, litigation and potential health & safety issues as well as service disruptions.	Failure to monitor contractors appropriately.	3	3	9	Finance Team Manager. All Team Managers.	All Heads of Service	Oversight Board structure in place to oversee major project work & compliance group now in place to oversee these elements of contracted work.	2	3	6	Stable
			Legal and procurement teams not consulted when contractors are engaged.						Corporate procurement support and legal team to support where necessary on contract management.				
			Loss of key staff or supplier.						Recasting procurement functions activity, processes and focus of training and education for staff in 2023				
			Procurement procedures are not followed.						Analysis of spend undertaken and procurement toolkit to be produced to cover majority of lower value procurements with high value and complex procurements to be supported by specialised function.				
			The council contributes to modern slavery via it's contracts and supplies.										
	5 LEGAL / TECHNOLOGICAL Loss or unlawful use of personal data constituting breach of data protection legislation	Monetary penalties from ICO, adverse publicity, private litigation and personal criminal liability of officers.	Systems not in place to protect sensitive data.	4	3	12	Legal Services Team Manager	Head of Legal & Support Services	Policies and procedures are in place and rolled out. Regularly reviewed and compliance is monitored.	2	2	4	Stable
			Staff are not properly trained in managing information, and do not follow internal procedures.						Corporate Governance training is undertaken annually and includes information governance as appropriate to reflect changes in legislation. E-learning module updated and rolled out as mandatory annual training for all staff.				
			Changes in working practises causing unintended risk/exposure						The Council has a dedicated SIRO and DPO.				
									Corporate Governance Groups are in place to scrutinise impacts/issues arising.				

Corporate Risk Register													
Ref No.	Risk Description	Consequence	Cause	Inherent Risk			Responsibility of	Responsible to	Control Measures	Residual Risk			Movement of Risk
				Impact	Likelihood	Rating				Impact	Likelihood	Rating	
									Internal audit was carried out in December 2019. The outcome of the audit was a Grade 1. One medium risk recommendation				
									Information Governance Team to cooperate with the supervisory authority and monitor compliance with Data Protection laws.				
6	LEGAL / REPUTATIONAL / COMMERCIAL Failure to respond to an emergency in an appropriate manner	General public at risk of harm or unable to access relevant services (e.g. emergency accommodation or rest centre).	Lack of planning, training and exercising of Emergency plans	4	3	12	Head of Human Resources and Organisation Development	Chief Executive	Business continuity plans have been documented, policies and procedures are in place. LRF and Council resilience discussions to consider plans in light of possible impacts of power outages. Exercises local and national planned in early 2023	4	1	4	Stable
		Adverse publicity. "Business as usual" not possible without appropriate business continuity plan in place.	Inadequate Corporate Business Continuity Management.						The LRF partnership arrangement with all Leicestershire and Rutland authorities provide resilience during civil emergency situations.				
		Breakdown in relationship with other responders.	Lack of procedural understanding						Business Continuity exercises show the readiness of the Council to deal with emergencies. System of ICO / FLM duty rotas is in place & continued reassessment for ongoing incidents. COVID experience shows capability and ability to perform.				
7	LEGAL/ TECHNOLOGICAL/ COMMERCIAL Infiltration of ICT systems	"Business as usual" would not be possible. Cost of repelling cyber threat and enhancing security features.	Systems not in place or kept current to deflect any foreseeable cyber attack.	4	4	16	ICT Manager	Directors. Chief Executive.	Fully resilient environment in place with no single points of failure for core systems, other critical systems use cold standby equipment.	3	2	6	Stable
17			Limited staff awareness of possible threats.						Yearly IT security health check and PEN (penetration) testing carried out, by a CREST security accredited supplier, with remediation action plan in place to mitigate any risks found. In 2023 we had 0 critical, 0 high, 4 medium and 8 Low issues, which have now been remediated.				
			Lapse in security awareness and basic processes from a technical and human perspective.						Phishing campaigns ran twice a year to test staff security awareness and feed back results to CLT, with improvement plans in place for those who have not passed the test.				
									Quarterly Cyber Security awareness training held for staff and new starters, to protect staff at work and in the office.				
									New business services are run in remote fully resilient data centres and existing systems are being progressively migrated to these cloud computing centres.				
									Diversity of environments used to avoid single point of failure risk				
									Improved business recovery arrangements have been implemented to minimise recovery time.				
									Accreditation to Cyber Essentials and the Public Services Network.				
									Latest Audit / assessments all confirm secure environment with reasonable assurance. Some formalisation of processes required and review of backups restoration window.				

Corporate Risk Register													
Ref No.	Risk Description	Consequence	Cause	Inherent Risk			Responsibility of	Responsible to	Control Measures	Residual Risk			Movement of Risk
				Impact	Likelihood	Rating				Impact	Likelihood	Rating	
									An annual external audit of IT assessed the organisation's IT arrangements in a range of areas against best practice. The outcome of the audit in 2023 was, reasonable assurance, with 3 high recommendations and 4 mediums, mainly around backup and formalisation of processes, plans have been put in place to address these and provides assurance that the organisation's IT arrangements are solid, sound and secure.				
8	COMMERCIAL / POLITICAL / FINANCIAL Projects are poorly managed	Failure of proposed projects could result in failure to achieve overall objectives. Inefficient use / waste of resources.	Failure to implement project management techniques. Poor corporate oversight of projects. Inadequate controls on expenditure and poor budget monitoring.	3	3	12	Strategic Directors	Chief Executive	Greater use of professional project managers for key projects. Work ongoing to address project methodologies deployed across the council. Greater use of external / out of subject board members. Board structure covering all major projects in place	3	2	6	Stable
			Properly convened project teams with PID and project plan in place, including project risk registers. Progress on corporate projects scrutinised by CLT. Implementation of contract management framework for outsourced services. Scrutiny of quarterly monitoring reports on capital expenditure.										
18			Utilising Internal Audit to conduct audits of individual projects or Project management more widely. Use of external resources to be used to support the major projects. Scrutiny of risk registers or project management framework of individual projects by Risk Scrutiny Group. 2022 audit has identified areas of weakness in controls and upon implementation of these the risk will be reduced and therefore these will continue to be monitored										
9	LEGAL / POLITICAL / REPUTATIONAL Council makes ultra vires (beyond the council's powers and functions) decisions or those which it does not have the correct permissions to undertake	Potential litigation against the Council, resulting in increased costs / compensation. Reputational damage.	Staff / Members proceeding without established governance arrangements. Failure to consult with Legal / Monitoring Officer. Lack of understanding of the implications of dealing with a particular matter or conditions of service delivery.	4	3	12	Legal Services Team Manager & Service Managers	Head of Legal & Support Services	Policies & procedures in place, governance processes are documented and in operation, ongoing assessments and reviews are performed. Completion of the Annual Governance statement.	4	1	4	Stable
10	FINANCIAL / LEGAL / REPUTATIONAL Council is subject to serious fraud, corruption or theft	Financial, reputational and political damage to Council.	Lack of checks and balances within financial regulations.	4	3	12	Head of Finance. All Team Managers & Heads of Service.	Directors		3	2	6	Stable
			Poor budget / contract management.						A policy framework that includes Anti-Fraud and Corruption Policy, Confidential Reporting (Whistleblowing) Policy and Anti-Money Laundering Policy. Policy Refreshed late 2020 - refresh of training underway.				

Corporate Risk Register													
Ref No.	Risk Description	Consequence	Cause	Inherent Risk			Responsibility of	Responsible to	Control Measures	Residual Risk			Movement of Risk
				Impact	Likelihood	Rating				Impact	Likelihood	Rating	
			Poor monitoring of / adherence to financial systems						The Internal Audit annual planning process takes into account high risk areas, which considers fraud risks. Fraud risks are considered as part of specific audits with testing designed to detect fraud where possible. The Council is also subject to External Audit. New Covid related Grants all subject to external audit and compliance checks.				
			Changes in working practises casuing unintended risk/exposure						Internal control and governance arrangements such as segregation of duties, schemes of delegation, bank reconciliations of fund movements, and verification processes.				
									Participation and strengthening of involvement in National Fraud Initiative (mandatory) Information on how to report fraud is on the website including relevant links.				
19	11 FINANCIAL / COMMERCIAL / ECONOMIC The Council is subject to a reduction in income long term	Services are unable to be delivered. Potential staff redundancies. Funding of external groups is withdrawn. Potential breach of statutory duties/ability to delvier objectives compromised	Gov plans reduction in business rates share to NWL. Changes to the local authority financial settlement. Economic downturn / recession. Commercial opportunities not progressed. Changing rent policies.	4	4	16	Head of Finance. All Heads of Service.	Directors. Chief Executive.	Medium Term Financial Strategy in place, and will be reviewed at key events. Change in budgeting focus from incremental to outcomes focussed expected to identify quick wins and pland for longer term self-sufficiency. Head of Finance monitoring of Local Government funding reviews. Funding advisor engaged. Economic Development Team promotes business offer. Participation in Business Rates Pooling. Accessing external funding where appropriate. Income collection procedures in Revs & Bens Service and Housing sound. Leicestershire Revenues and Benefits Partnership have two trained officers working solely on Council Tax Reduction Scheme Fraud and act as Single Point of Contact for DWP referrals.	2	3	6	Stable
	12 POLITICAL / ORGANISATIONAL The Council is affected by Local Government Reorganisation	a) Change to Local Government structure in Leicestershire/East Midlands, including potential merger of district councils/county council or development of a Combined Authority for the East Midlands, or elected Major either of which could lead to: - Change in location for service delivery/staff - Reduction of control over local matters - Change in financial situation - Staff redundancies - Alternative political structure and governance arrangements - Changes in services to be provided and organisation culture - Deterioration in staff morale and negative effect on staff recruitment and retention - Ineffective engagement with staff, Members and residents in considering, and responding to, proposals. - Diversion of senior staff resources to respond to proposals.	Political direction to consolidate local government tiers to potentially seek greater efficiency and co-ordination	4	3	12	Chief Executive and Head of Legal and Support Services.	Chief Executive	Active engagement with political leaders and Chief Executives across the County and East Midlands so NWL's needs are taken into account in any proposals. Open and transparent communication of NWL position to all stakeholders. Senior management and politicians stay close to project and monitor progress. Internal and external communication plans in place, including for key decision points. Gov stance changed to no longer pursue wholesale LGR - County Deals not linked to LGR. Leicestershire Cat 2 County Deal	1	3	3	Stable

Corporate Risk Register													
Ref No.	Risk Description	Consequence	Cause	Inherent Risk			Responsibility of	Responsible to	Control Measures	Residual Risk			Movement of Risk
				Impact	Likelihood	Rating				Impact	Likelihood	Rating	
13	POLITICAL / ORGANISATIONAL The Council is affected by the UK's departure from the EU	The UK's departure from the EU, leads to impacts on supply of goods, staff, services generally. Specifically increase in checks on goods by Environmental Officers at East Midlands Airport meaning increase in resources / costs.	UK departure from EU/Brexit	4	4	16	Chief Executive and Head of Economic Regeneration & Team Manager for Environmental Health	Directors & Chief Executive	Engage with National Local Authority steering groups for border control at strategic & operational levels. Implement communication strategy for local businesses so technical notices are shared, with appropriate signposting. Work with LLEP and Chamber of Commerce to provide business advice and support to address changes to legislation & certification. Watching brief localised assessment of potential impact around East Midlands Airport. Participate in Multi-agency Leicestershire Resilience Forum framework, with risk assessment and mitigation plan to be prepared. Applied for and gained additional support funding for Port activity	2	2	4	Stable
14	ORGANISATIONAL/FINANCIAL Council is subject to large scale and medium term reduction in staffing/supplies/increase in restrictions etc leading to risks and ongoing medium/long term impacts on either the financial or reputational standing of the Council	Financial, reputational and political damage to Council.	Pandemic, national/global infrastructure interruption, supply chain mass failure over medium / long time period	4	4	16	Chief Executive, Directors, Heads of Service	Chief Executive	Balanced budget achieved with additional government grant support. Continued active engagement and lobbying to ensure that all options for support are considered and actioned where possible. COVID 19 experience has led to myriad of changes to make service provision more robust. Further mitigations for other similar events in place - eg promotion of vaccinations, system readiness and deployment remotely, updating Business Continuity plans etc Engagement with LRF processes and training	2	2	4	Stable
15	ORGANISATIONAL//POLITICAL No overall control of the Council following the May 2023 elections could lead to instability in the decision making process which could impact adversely on service delivery	Financial, reputational and political damage to the Council. Slower decision making.	The election in May 2023 changed the political make up of the Council	3	3	9	Chief Executive, Directors, Heads of Service	Chief Executive	There has been extensive work by officers to work with all Groups to minimise the impact. This work has been supplemented by external engagement with the Local Government Association. The work undertaken to date includes: regular briefings with all Groups, a member induction programme, a continuing training programme for councillors, clarity on the roles of councillors on each committee and engaging with staff to raise their awareness in dealing with/responding to/working with councillors.	2	3	6	New Risk
16	ORGANISATIONAL/REPUTATIONAL There is greater focus from Government and regulators on the local government sector. There is a risk of an impact of an adverse external assessment on the Council. If this risk materialised it could impact on service delivery, performance levels, governance and	Financial, reputational, legal and political damage to the Council.	Greater focus on the local government sector from Government and regulators following high profile council 'failures'	4	2	8	Chief Executive, Directors, Heads of Service	Chief Executive	The Council has in place a range of controls including financial procedures, governance framework, performance management framework, project management methodology, strategies, controls underpinning its operations, clear communication with staff, Statutory officer meetings and internal audit plan. The Council is aware of the creation of the Office for Local Government and is actively working to understand the implications/requirements for the Council.	2	2	4	New Risk

Corporate Risk Register													
Ref No.	Risk Description	Consequence	Cause	Inherent Risk			Responsibility of	Responsible to	Control Measures	Residual Risk			Movement of Risk
				Impact	Likelihood	Rating				Impact	Likelihood	Rating	
17	SOCIAL/POLITICAL/REPUTATIONAL - Climate Change / Zero Carbon delivery	The failure of the Council to Council to achieve carbon neutrality for its operations by 2030 and carbon neutrality for the District by 2050. This may have long term impacts on both the financial picture of the council and the ability of key service provision in the long term.	Inability to deliver programme due to resource / financial / operational / proecdural process. Inability to gain action by partners	3	4	12	Chief Executive, Directors, Heads of Service	Chief Executive	Achievement of the carbon reduction ambitions are mainly vested in our Climate and Environment Strategy and Zero Carbon Programme. The Action Plan contains planned and programmed actions and will be reviewed annually. It will quantify the estimated net financial costs and net carbon savings associated with the contents of the Plan. Attaining the targets in the Plan is one of the Corporate Plan Key Performance Indicators. Whilst the action plan has been agreed it does contain several actions where funding hasnot been committed. The Strategy and Plan have identified the main carbon	2	2	4	Stable

Corporate Risk Register													
Ref No.	Risk Description	Consequence	Cause	Inherent Risk			Responsibility of	Responsible to	Control Measures	Residual Risk			Movement of Risk
				Impact	Likelihood	Rating				Impact	Likelihood	Rating	

Assessing the likelihood of a risk:

1 Low	Likely to occur once in every ten years or more
2 Medium	Likely to occur once in every two to three years
3 High	Likely to occur once a year
4 Very high	Likely to occur at least twice in a year

1 Low	<p>Loss of a service for up to one day, Objectives of individuals are not met No injuries</p> <p>Financial loss below £10,000 No media attention No breaches in council working practices No complaints / litigation</p>
2 Medium	<p>Loss of a service for up to one week with limited impact on the general public Service objectives of a service unit are not met Injury to an employee or member of the public requiring medical treatment Financial loss over £10,000 Adverse regional or local media attention – televised or newspaper report Potential for a complaint litigation possible Breaches of regulations / standards</p>
3 High	<p>Loss of a critical service for one week or more with significant impact on the public and partner organisations Service objectives of the directorate of a critical nature are not met Non- statutory duties are not achieved Permanent injury to an employee or member of the public Financial loss over £100,000 Adverse national or regional media attention – national newspaper report Litigation to be expected Breaches of law punishable by fine</p>
4 Very high	<p>An incident so severe in its effects that a critical service or project will be unavailable permanently</p> <p>Strategic priorities of a critical nature are not met</p> <p>Statutory duties are not achieved Death of an employee or member of the public Financial loss over £1m. Adverse national media attention – national televised news report Litigation almost certain and difficult to defend Breaches of law punishable by imprisonment</p>

NORTH WEST LEICESTERSHIRE DISTRICT COUNCIL

AUDIT AND GOVERNANCE COMMITTEE – WEDNESDAY, 26
JULY 2023

Title of Report	TREASURY MANAGEMENT ACTIVITY REPORT - QUARTER 1 2023/24	
Presented by	Anna Crouch Head of Finance & Deputy S151 Officer	
Background Papers	Prudential Indicators and Treasury Strategies 2023-24	Public Report: Yes
Purpose of Report	To inform Members of the Council's Treasury Activity for the period April – June 2023.	
Recommendations	THAT MEMBERS APPROVE THIS REPORT AND COMMENT AS APPROPRIATE.	

1.0 BACKGROUND

- 1.1 Treasury Management activity is underpinned by the Chartered Institute of Public Finance and Accountancy's Treasury Management in the Public Services: Code of Practice (the CIPFA Code), which requires local authorities to produce Prudential Indicators and a Treasury Management Strategy Statement annually on the likely financing and investment activity. The Prudential Indicators and Treasury Strategies were approved by Council on the 23 February 2023.
- 1.2 As a minimum, the code requires that the council reports on the performance of the Treasury Management function at least twice yearly (mid-year and at year end). The Council reports on its treasury activities quarterly. Appendix A is the second of four reports to be presented in 2023/24 designed to inform Members of the council's treasury activity and enable scrutiny of activity and performance.

2.0 TREASURY MANAGEMENT ADVISORS' COMMENTARY – ARLINGCLOSE LTD

- 2.1 The commentary below has been provided by the Councils treasury management advisors:
- 2.2 NWLDC is currently taking a relatively low credit and liquidity risk approach to its investment strategy by investing mainly in deposits with UK central government, Money Market Funds (MMFs), UK local authorities, and a small number of UK banks, for short terms (up to 12 months). Most of these options avoid the direct bail-in risk associated

with bank deposits (although indirect exposure is held via the MMFs, this is highly diversified).

- 2.3 Interest rates have been rising globally and uncertainty remains over when major central bank policy rates will peak, in particular regarding how much further UK Bank Rate may increase given persistent inflation. The Council's investment returns have therefore increased but the level of real return (i.e. adjusting for inflation) is negative given current high inflation. The latest client investment benchmarking exercise that NWLDC took part in (March 2023) showed the council's return was slightly lower than the average for other local authorities but credit risk (as measured by credit ratings) was also lower, for internally managed investments.
- 2.4 Other investment options that may fit with the council's current risk appetite could include secured bank deposits (up to 12 months), longer-term loans to local authorities (the council has done this before), covered or supranational bonds and loans to Registered Providers (housing associations), which may also require a longer investment horizon (3 to 5 years).
- 2.5 Going beyond this would be an alternative approach – investing for the long-term (5 years +) in asset classes such as property, bonds and equities which fluctuate in value, and carry a different and typically higher set of risks but offer the potential for higher long-term returns. The Council would need to identify a long-term investment horizon and/or these types of investments may need to be part of a documented strategy to manage liquidity, interest rate, exchange rate and/or inflation risks.

3.0 SUMMARY

- 3.1 In compliance with the requirements of the CIPFA code of practice, Appendix A provides Members with a summary report of the Treasury Management activity for the period April 2022 to December 2022. A prudent approach has been taken in relation to investment activity with priority being given to security and liquidity over yield.
- 3.2 For the reporting period, there has been one breach of the Treasury Management Strategy Statement that need bringing to the attention of the committee outlined in the following report

Policies and other considerations, as appropriate	
Council Priorities:	<p>The Treasury Strategies and Prudential Indicators help the Council achieve all its properties:</p> <ul style="list-style-type: none"> - Supporting Coalville to be a more vibrant, family-friendly town - Support for businesses and helping people into local jobs - Developing a clean and green district - Local people live in high quality, affordable homes - Our communities are safe, healthy and connected
Policy Considerations:	Not applicable
Safeguarding:	Not applicable
Equalities/Diversity:	Not applicable
Customer Impact:	Not applicable
Economic and Social Impact:	Not applicable
Environment and Climate Change:	Not applicable
Consultation/Community Engagement:	Not applicable
Risks:	Borrowing and investment both carry an element of risk. This risk is mitigated through the adoption of the Treasury and Investment Strategies, compliance with the CIPFA code of Treasury Management and the retention of Treasury Management advisors (Arlingclose) to proffer expert advice.
Officer Contact	<p>Anna Crouch Head of Finance & Deputy S151 Officer anna.crouch@nwleicestershire.gov.uk</p>

This page is intentionally left blank

Treasury Management Activity Report Quarter 1 2023/24**1. Introduction**

- 1.1 The Authority has adopted the Chartered Institute of Public Finance and Accountancy's Treasury Management in the Public Services: Code of Practice (the CIPFA Code) which requires the Authority to approve treasury management semi-annual and annual reports.
- 1.2 This quarterly report includes the new requirement in the 2021 Code, mandatory from 1st April 2023, of quarterly reporting of the treasury management prudential indicators.
- 1.3 The Authority's treasury management strategy for 2023/24 was approved at a Council meeting on 23 February 2023. The Authority has invested substantial sums of money and is therefore exposed to financial risks including the loss of invested funds and the revenue effect of changing interest rates. The successful identification, monitoring and control of risk remains central to the Authority's treasury management strategy.

2. External Context (provided by Arlingclose)

- 2.1 Economic background: From the start of the quarter until May it looked like peak global monetary policy rates were in sight as inflation continued to ease and central banks turned more dovish in tone. Only a few weeks later, stronger and more persistent inflation data, particularly in the UK, changed the picture.
- 2.2 The UK situation was not welcome news for the Bank of England. GDP growth was weak, confirmed at 0.1% in Q1, although more recent monthly GDP data has been somewhat better. The housing market has stalled, consumer demand is weak but seemingly recovering despite higher interest rates, and labour demand remained strong, with repercussions for wage growth which is accelerating.
- 2.3 April data showed the unemployment rate increased to 3.8% (3mth/year) while the employment rate rose to 76.0%. Pay growth was 6.5% for total pay (including bonuses) and 7.2% for regular pay, the largest growth rate of the latter outside of the Covid pandemic. Once adjusted for inflation, however, growth in total pay and regular pay remained negative.
- 2.4 Inflation fell from its peak of 11.1% reached in October 2022, but annual headline CPI in May 2023 was higher than the consensus forecast at 8.7% (8.4% expected), largely driven by services inflation, while the annual measure of underlying core inflation rose to 7.1% from 6.8%.
- 2.5 After a sharp rise in interest rate expectations, with clearly serious implications for mortgage markets due to higher inflation and wage data, the Bank of England's Monetary Policy Committee reaccelerated monetary policy tightening over the period with a 0.25% rise in May to a 0.5% rise in June, taking Bank Rate to 5.0%. At both meetings the vote was 7-2 in favour of increasing rates, with the two dissenters preferring to keep rates on hold.
- 2.6 Interest rate expectations priced in further hikes in policy rates. Arlingclose, the authority's treasury adviser, revised its forecast to forecast a further 0.5% of monetary tightening to take Bank Rate to 5.5%. The risks, however, are that rates could be higher; financial markets are

forecasting policy interest rates above 6%.

- 2.7 With many mortgages at low fixed rates now systematically being re-set over the next 12-24 months at higher rates at the end of their fixed rate period, there has been a lagged effect of the feed through of monetary policy on households' disposable income. The economic slowdown is expected to develop over time and therefore, despite the GfK measure of consumer confidence rising to -24 in June, it is likely confidence will be negatively affected at some point. The manufacturing sector contracted during the quarter according to survey data, which will eventually feed into services, whose expansion is slowing.
- 2.8 Despite the US Federal Reserve increasing its key interest rate to 5.00-5.25% over the period, activity in the region continued to defy monetary tightening, particularly in labour markets which have so far appeared robust, supporting the Fed's assertions of two more rate hikes after it paused in June. Annual US inflation continued to ease, falling from 4.9% in April to 4.0% in May, the lowest level since March 2021. US GDP growth at 2% annualised in the first calendar quarter of 2023 was also significantly stronger than expected against the initial estimate of 1.3%.
- 2.9 In the euro zone, the picture was somewhat different. The European Central Bank maintained its hawkish tone and increased its key deposit, main refinancing, and marginal lending interest rates to 3.50%, 4.00% and 4.25% respectively. There were signs of weakening activity, particularly in Germany whose manufacturing sector has taken a hit from high energy prices and weaker global demand. However, inflation remained sticky, annual headline CPI fell to 5.5% in June while annual core inflation rose to 5.4% from 5.3%, which means the ECB is unlikely to stop monetary tightening.
- 2.10 Financial markets: Financial market sentiment and bond yields remained volatile, the latter continuing their general upward trend as uncertainty and concern over higher inflation and higher interest rates continued to dominate.
- 2.11 Gilt yields rose over the period. The 5-year UK benchmark gilt yield rose from 3.30% to 4.67%, the 10-year gilt yield from 3.43% to 4.39%, and the 20-year yield from 3.75% to 4.51%. The Sterling Overnight Rate (SONIA) averaged 4.37% over the quarter.
- 2.12 Credit review: Having completed a review of its credit advice on unsecured deposits at UK and non-UK banks following concerns of a wider financial crisis after the collapse of Silicon Valley Bank purchase of Credit Suisse by UBS, as well as other well-publicised banking sector issues, in March Arlingclose reduced the advised maximum duration limit for all banks on its recommended counterparty list to 35 days.
- 2.13 Over the period S&P upgraded NatWest Group and related entities to A+ (except NatWest Markets which was upgraded to A), revised the UK sovereign outlook to stable from negative, and upgraded both Barclays Bank PLC and Barclays Bank UK PLC to A+.
- 2.14 Fitch put the US sovereign rating on Rating Watch Negative following increased political partisanship which at the time was hindering the latest resolution to raise the debt ceiling. It also upgraded the outlook on United Overseas Bank to stable, the outlook on Clydesdale to positive, and the outlook on Bank of Montreal to stable.
- 2.15 Moody's withdrew Guildford BC's rating (who chose not to continue being rated) and affirmed the Aaa rating of the European Investment Bank.

- 2.16 Arlingclose continued to monitor and assess credit default swap levels for signs of ongoing credit stress but made no changes to the counterparty list or recommended durations over the quarter. Nevertheless, heightened market volatility is expected to remain a feature, at least in the near term and, as ever, the institutions and durations on the Authority's counterparty list recommended by Arlingclose remains under constant review.

3. Local Context

- 3.1 On 30th June 2023, the Authority had net borrowing of £9.6m arising from its revenue and capital income and expenditure. The underlying need to borrow for capital purposes is measured by the Capital Financing Requirement (CFR), while usable reserves and working capital are the underlying resources available for investment. These factors are summarised in Table 1 below.

Table 1: Balance Sheet Summary

	31.3.23 Estimated £m
General Fund CFR	38.5
HRA CFR	56.6
Total CFR	95.2
External borrowing	62.6
Internal borrowing	32.6
Total Borrowing	95.2

- 3.2 The treasury management position on 30 June 2023 and the change over the preceding three months is shown in Table 2 below.

Table 2: Treasury Management Summary

	31.3.23 Balance £m	Movement £m	30.06.23 Balance £m	30.06.23 Rate %
Long-term borrowing	59.8	0.0	59.8	3.6%
Short-term borrowing	2.7	0.0	2.7	4.2%
Total borrowing	62.6	0.0	62.6	3.6%
Long-term investments	0.0	0.0	0.0	0.0%
Short-term investments	39.0	-4.0	35.0	4.6%
Cash and cash equivalents	4.1	13.9	18.0	4.7%
Total investments	43.1	9.9	53.0	4.7%
Net borrowing	19.5	-9.9	9.6	

4.0 Borrowing

- 4.1 CIPFA's 2021 Prudential Code is clear that local authorities must not borrow to invest primarily for financial return and that it is not prudent for local authorities to make any investment or spending decision that will increase the capital financing requirement, and so may lead to new borrowing, unless directly and primarily related to the functions of the Authority.
- 4.2 PWLB loans are no longer available to local authorities planning to buy investment assets primarily for yield the Authority intends to avoid this activity in order to retain its access to PWLB loans.
- 4.3 The Authority currently holds £8.9m in commercial investments that were purchased prior to the change in the CIPFA Prudential Code. These commercial investments are primarily for local regeneration and growth with a secondary objective of financial return. Before undertaking further additional borrowing the Authority will review the options for exiting these investments.
- 4.4 As shown in table 1 the authority has internally borrowed £32.6m. This internal borrowing foregoes a potential interest income rate of 4.7%. Current one year external borrowing rates with the PWLB are 6.4% as at 30 June 2023. An additional rate for HRA specific borrowing has been implemented from June 2023 which is 0.4% lower than standard PWLB rates.

5. Borrowing Strategy and Activity

- 5.1 As outlined in the treasury strategy, the Authority's chief objective when borrowing has been to strike an appropriately low risk balance between securing low interest costs and achieving cost certainty over the period for which funds are required, with flexibility to renegotiate loans should the Authority's long-term plans change being a secondary objective. The Authority's borrowing strategy continues to address the key issue of affordability without compromising the longer-term stability of the debt portfolio.
- 5.2 There has been a substantial rise in the cost of both short- and long-term borrowing over the last 18 months. In this quarter, Bank Rate rose from 4.25% at the beginning of April to 5.0% at the end of the quarter and was also significantly higher than its level of 1.25% at the end of June 2022.
- 5.3 Gilt yields faced upward pressure since early April following signs that UK growth has been more resilient and inflation stickier than expected. Consequently, PWLB borrowing rates continued to rise over the quarter. On 30th June, the PWLB certainty rates for maturity loans were 5.25% for 10 year loans, 5.36% for 20-year loans and 4.95% for 50-year loans. Their equivalents on 31st March 2023 were 4.33%, 4.70% and 4.41% respectively.
- 5.4 A new PWLB HRA rate which is 0.4% below the certainty rate has been made available from 15th June 2023. Initially available for a period of one year, this discounted rate is to support local authorities borrowing for the Housing Revenue Account and for refinancing existing HRA loans, (add, if applicable) providing a window of opportunity for HRA-related borrowing.
- 5.5 As the Council has not undertaken any new borrowing this financial year the effects of these rate rises have not been felt. However, should the Council decide to borrow in the next year this effect will increase the cost of borrowing.

- 5.6 At 30th June 2023 the Authority held £62.6m in loans, there has been no decrease since 31st March 2023 as no principle has yet been repaid this year. A breakdown of outstanding loans is shown below in table 3.

Table 3: Borrowing Position

	31.3.23 Balance £m	Net Movement £m	31.06.23 Balance £m	31.06.23 Weighted Average Rate %	31.06.23 Weighted Average Maturity (years)
Public Works Loan Board	55.1	0.0	55.1	3.4%	15.7
Banks (LOBO)	3.5	0.0	3.5	4.8%	31.6
Banks (fixed-term)	3.9	0.0	3.9	4.7%	30.6
Local authorities (long-term)	0.0	0.0	0.0	0.0%	0.0
Local authorities (short-term)	0.0	0.0	0.0	0.0%	0.0
Total borrowing	62.6	0.0	62.6	0.0	17.5

- 5.7 There remains a strong argument for diversifying funding sources, particularly if rates can be achieved on alternatives which are below gilt yields + 0.80%. The Authority will evaluate and pursue these lower cost solutions and opportunities with its advisor Arlingclose.
- 5.8 The Authority has £3.5m LOBO loans with call dates within the next 12 months on the 8 August 2023 and 8 February 2024. The Authority has liaised with their treasury management advisors Arlingclose over the likelihood of the options being exercised. If the option is exercised the Authority plans to repay the loan at no additional cost. If required, the Authority is likely to repay the LOBO loans with available cash. It may then consider replacing this in the future with external borrowing if interest rates are advantageous.
- 5.9 As interest rates increase there is an increased chance that the LOBO loan held by the authority will be called. The Council recently calculated that the chance of this occurring is still low at about 10% likelihood.

6. Treasury Investment Activity

- 6.1 CIPFA published a revised Treasury Management in the Public Services Code of Practice and Cross-Sectoral Guidance Notes on 20th December 2021. These define treasury management investments as investments that arise from the organisation's cash flows or treasury risk management activity that ultimately represents balances that need to be invested until the cash is required for use in the course of business.
- 6.2 The Authority holds significant invested funds, representing income received in advance of expenditure plus balances and reserves held. During the year, the Authority's investment balances have ranged between £43.3m and £57.7m million due to timing differences between income and expenditure. The investment position is shown in table 4 below.

Table 4: Treasury Investment Position

	31.3.23	Net	30.06.2023	30.06.2023	30.06.2023
	Balance	Movement	Balance	Income	Weighted
	£m	£m	£m	Return	Average
				%	Maturity
					days
Banks & building societies (unsecured)	2.0	0.0	2.0	4.5%	1.3
Government (incl. local authorities)	37.0	-4.0	33.0	4.6%	86.8
Money Market Funds	4.1	13.9	18.0	4.7%	0.3
Total investments	43.1	9.9	53.0	4.7%	88.5

- 6.3 The above graph shows an increase in total investment balances since 31 March 2023. This notable increase can be partly attributed to the timing of receipts received by the Council, where funds were acquired before being utilized for payments. Moreover, the accumulation of investment balances can also be attributed to various other factors. One such factor is the potential slippage in the capital programme, where delays or project complexities result in unutilized funds. Additionally, the Council planning to accumulate reserves for future use, enhancing financial stability and preparedness.
- 6.4 Both the CIPFA Code and government guidance require the Authority to invest its funds prudently, and to have regard to the security and liquidity of its treasury investments before seeking the optimum rate of return, or yield. The Authority's objective when investing money is to strike an appropriate balance between risk and return, minimising the risk of incurring losses from defaults and the risk of receiving unsuitably low investment income.
- 6.5 As demonstrated by the liability benchmark in this report, the Authority expects to be a long-term borrower and new treasury investments are therefore primarily made to manage day-to-day cash flows using short-term low risk instruments. The existing portfolio of strategic pooled funds will be maintained to diversify risk into different sectors and boost investment income.
- 6.6 Bank Rate increased by 0.75%, from 4.25% at the beginning of April to 5% by the end of June, with the prospect of further increases to come. Short-dated cash rates rose commensurately, with 3-month rates rising to around 5.25% and 12-month rates to nearly 6%. The rates on DMADF deposits also rose, ranging between 4.8% and 5.4% by the end of June and Money Market Rates between 4.7% and 4.8%.
- 6.7 The progression of risk and return metrics are shown in the extracts from Arlingclose's quarterly investment benchmarking in Table 5 below.

Table 5: Investment Benchmarking – Treasury investments managed in-house*

	Credit Score	Credit Rating	Bail-in Exposure	Weighted Average Maturity (days)	Rate of Return %
31.03.2023	4.07	AA-	14%	78	3.49%
Similar Las	4.74	A+	63%	56	0.73%
All Las	4.71	A+	59%	12	1.59%

**From last available benchmarking data*

- 6.8 The Authority has budgeted £795,000 in interest income from investments after deductions in 2023/24. Actual income received by June 30 2023 was £539,000. We are now forecasting the risk adjusted interest received by March 31 2024 to be £1.5m and after deductions income to be £1.2m.
- 6.9 Interest rates can and have been extremely volatile over the financial year and are likely to be similarly volatile in the upcoming months. Therefore, for the purpose of budget setting these forecasts are reduced by 20% to ensure that there is not an overreliance placed on interest return for creating a balanced budget.
- 6.10 The updated forecast of £1.2m will be split between the General Fund (GF) and Housing Revenue Account (HRA). This split will be 51% to the GF and 49% to HRA. The percentage split is worked using the investment balances for both funds throughout the year as a percentage of the overall investment fund. This is subject to change.
- 6.11 Interest forecasts are notoriously difficult to predict and are subject to change particularly in an unstable interest rate environment and constantly changing economic environment. The increase from £795,000 forecasted to £1.2m forecasted is as a result of this changing economic situation and also as a result of the Council having higher investment balances than expected due to delayed repayment of Covid Grants, Business rates levy and S31 funds and slippage in capital programmes. These factors have both boosted the Councils overall Treasury Balances and the return received on investments.

7. Non-Treasury Investments

- 7.1 The definition of investments in CIPFA's revised 2021 Treasury Management Code covers all the financial assets of the Authority as well as other non-financial assets which the Authority holds primarily for financial return. Investments that do not meet the definition of treasury management investments (i.e. management of surplus cash) are categorised as either for service purposes (made explicitly to further service objectives) and or for commercial purposes (made primarily for financial return).
- 7.2 Investment Guidance issued by the Department for Levelling Up Housing and Communities (DLUHC) and Welsh Government also includes within the definition of investments all such assets held partially or wholly for financial return.
- 7.3 The Authority held £8.9m of investments made for commercial purposes. This consisted entirely of directly owned property and land. A full list of the Authority's non-treasury investments is available in the Investment Strategy 2023-24 document. These investments are forecasted to generate £395,000 in investment income in 23/24 for the Authority after taking account of direct costs.
- 7.4 The main purpose of these investments is regeneration of the local area rather than investment income. All commercial investments are located within the District.

8. Treasury Performance

- 8.1 The Authority measures the financial performance of its treasury management activities both in terms of its impact on the revenue budget and its relationship to benchmark interest rates.

- 8.2 Since the beginning of the reporting period the Council has paid £81,000 in interest on borrowing. The forecasted amount to be spent on interest on loans for the financial year 23/24 in total is £2.2m. The overall interest rate on borrowing is 3.6%. For comparison purposes the current PWLB Maturity Loan rate for new 10 year borrowing is 6.4%. This represents a good rate of borrowing in the current environment
- 8.3 During the reporting period the Council has not yet paid back any principle on its loans. It is forecasting to repay £2.7m in PWLB loan principle by the end of the year. £1.2m of this is annuity loans whereby regular payments are made throughout the lifetime of the loan and the other is a maturity loan of £1.5m. There is no intention to borrow to replace these loans as the Council currently has the resources to absorb this.
- 8.4 The Council does not expect to undertake any new borrowing in the 2023/24 financial year and none has so far been undertaken.
- 8.5 As discussed in section 6.7 investment interest income during the reporting period was £538,000 before deductions. The Councils Investment interest return percentage on 30 June 2023 was 4.7%. For comparison purposes the Daily Sterling Overnight Index Average (SONIA) which is used for benchmarking purposes was 4.9%. For similar local authorities the most recent benchmarking data which is from 31 March 2023 showed an investment return of 0.73% largely due to the poor performance of external funds in which North West Leicestershire District Council is not involved. This is shown in Appendix 1.

9. **Compliance**

- 9.1 The S151 Officer reports that all treasury management activities undertaken during the quarter complied fully with the CIPFA Code of Practice. There was one breach of the Authority's approved Treasury Management Strategy whereby overnight £5.5m remained in the authorities bank account. The limit on overnight amounts kept in the account is £2.5m in the TMSS. This breach was a result of an investment being returned to the Councils bank account after dealing was completed for the day. Although this is a breach of the TMSS the funds remained in the Councils own bank account so exposure to risk was minimal. Steps have been put into place to ensure this is not repeated.
- 9.2 Compliance with the authorised limit and operational boundary for external debt is demonstrated in table 5 below.

Table 5: Debt Limits

	Q1 Maximum During Period	30.06.23 Actual	2023/24 Operational Boundary	2023/24 Authorised Limit	Complied?
Borrowing	£62.6m	£62.6m	£95.1m	£105.1m	Yes

- 9.3 Since the operational boundary is a management tool for in-year monitoring it is not significant if the operational boundary is breached on occasions due to variations in cash flow, and this is not counted as a compliance failure. However, there were no days in the reporting period in which the operational boundary was breached.

Table 6: Investment Limits

	Q1 Maximum	30.06.2023 Actual	2023/24 Limit	Complied?
The UK Government	£33.5m	£28m	Unlimited	Yes
Local authorities & other government entities	£9m	£5m	£60m	Yes
Secured investments	£0m	£0m	£60m	Yes
Banks (unsecured)	£2m	£2m	£60m	Yes
Building societies (unsecured)	£0m	£0m	£5m	Yes
Registered providers (unsecured)	£0m	£0	£12.5m	Yes
Money market funds	£22m	£18m	£60m	Yes
Strategic pooled funds	£0m	£0	£25m	Yes
Real estate investment trusts	£0m	£0	£12.5m	Yes
Other investments	£0m	£0	£2.5m	Yes

10. Treasury Management & Prudential Indicators

- 10.1 The Authority measures and manages its exposures to treasury management risks using the following indicators.
- 10.2 **Security:** The Authority has adopted a voluntary measure of its exposure to credit risk by monitoring the value-weighted average credit rating of its investment portfolio. This is calculated by applying a score to each investment (AAA=1, AA+=2, etc.) and taking the arithmetic average, weighted by the size of each investment. Unrated investments are assigned a score based on their perceived risk.

	31.03.23 Actual	2023/24 Target	Complied?
Portfolio average credit rating	AA-	A-	Yes

**From last available benchmarking data*

- 10.3 **Liquidity:** The Authority has adopted a voluntary measure of its exposure to liquidity risk by monitoring the amount of cash available to meet unexpected payments within a rolling three-month period, without additional borrowing.

	30.06.23 Actual	2023/24 Target	Complied?
Total cash available within 3 months	£24m	£2.5m	Yes

- 10.4 **Interest Rate Exposures:** This indicator is set to control the Authority's exposure to interest rate risk. The upper limits on the one-year revenue impact of a 1% rise or fall in interests was:

Interest rate risk indicator	30.06.23 Actual	2023/24 Limit	Complied?
Upper limit on one-year revenue impact of a 1% <u>rise</u> in interest rates	386,155	-600,000	Yes
Upper limit on one-year revenue impact of a 1% <u>fall</u> in interest rates	-386,155	-600,000	Yes

- 10.5 The impact of a change in interest rates is calculated on the assumption that maturing loans and investment will be replaced at current rates. Due to the majority of our investments maturing in year and the majority of our borrowing maturing in later years this means that we would benefit from an increase in Interest rates (as we replace investments with higher rates but not borrowing) but are negatively impacted by a decrease in interest rates for the same reason.
- 10.6 This is demonstrated in the above figures which show a positive return from an increase and a negative return from a decrease in interest rates. Both of these impact are within reasonable limits for the revenue budget. The Council also takes further precautions by reducing its interest forecast by a risk adjusted amount of 80% as discussed in paragraph 6.8.
- 10.7 For context, the changes in interest rates during the quarter were:

	31/3/23	30/6/23
Bank Rate	4.25%	5.00%
1-year PWLB certainty rate, maturity loans	4.78%	6.22%
5-year PWLB certainty rate, maturity loans	4.31%	5.71%
10-year PWLB certainty rate, maturity loans	4.33%	5.25%
20-year PWLB certainty rate, maturity loans	4.70%	5.36%
50-year PWLB certainty rate, maturity loans	4.41%	4.95%

- 10.8 **Maturity Structure of Borrowing:** This indicator is set to control the Authority's exposure to refinancing risk. [This indicator covers the risk of replacement loans being unavailable, not interest rate risk.] The upper and lower limits on the maturity structure of all borrowing were:

	30.06.23 Actual £m	30.06.23 Actual %	Upper Limit	Lower Limit	Complied?
Under 12 months	6.2	10%	70%	0%	Yes
12 months and within 24 months	1.3	2%	30%	0%	Yes
24 months and within 5 years	3.2	5%	30%	0%	Yes
5 years and within 10 years	2.5	4%	90%	0%	Yes
10 years and within 20 years	43.8	70%	90%	0%	Yes
20 years and above	5.7	9%	30%	0%	Yes

- 10.9 Time periods start on the first day of each financial year. The maturity date of borrowing is the earliest date on which the lender can demand repayment. As the LOBO functions this way an additional £3.5m is included in the under 12 months section and removed from the 20

years and above section despite the LOBO maturing in 2055.

- 10.10 **Principal Sums Invested for Periods Longer than a year:** The purpose of this indicator is to control the Authority's exposure to the risk of incurring losses by seeking early repayment of its investments. The limits on the long-term principal sum invested to final maturities beyond the period end were:

	2023/24	2024/25	2025/26	No Fixed Date
Actual principal invested beyond year end	£0	£0	£0	£0
Limit on principal invested beyond year end	£60m	£10m	£10m	£10m
Complied?	Yes	Yes	Yes	Yes

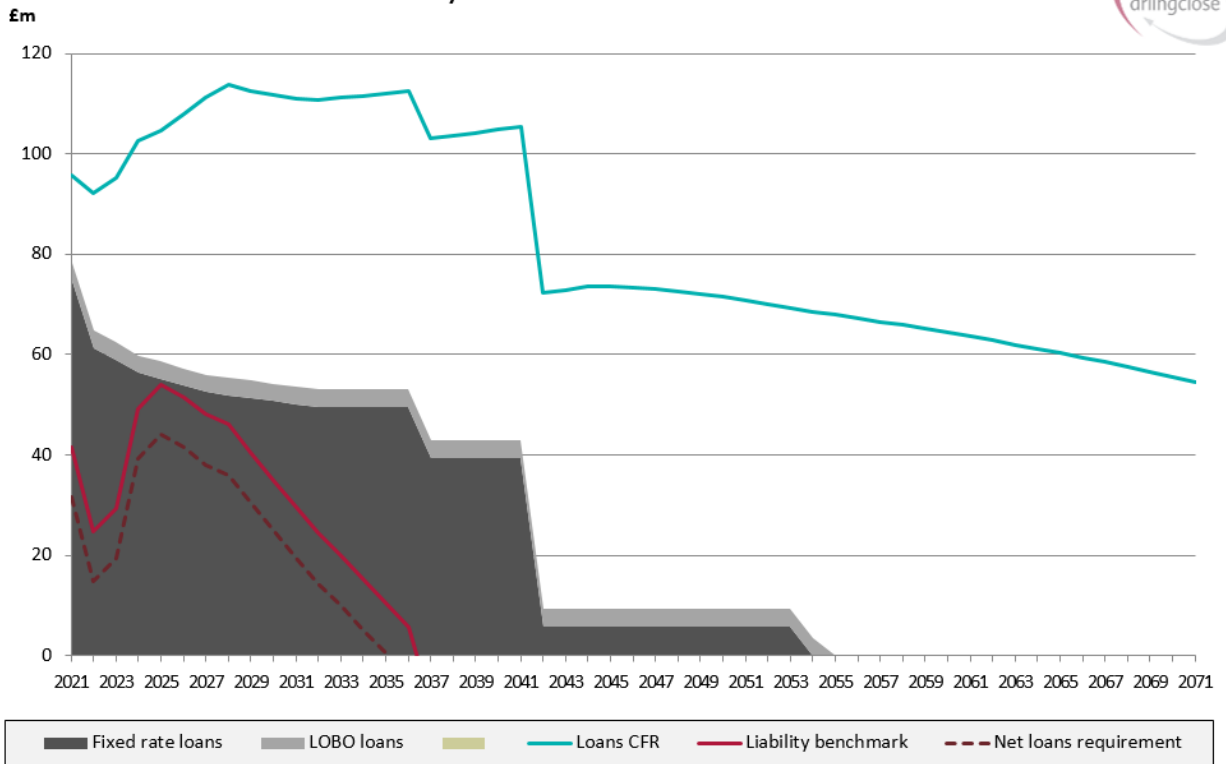
- 10.11 **Liability Benchmark:** This new indicator compares the Authority's actual existing borrowing against a liability benchmark that has been calculated to show the lowest risk level of borrowing. The liability benchmark is an important tool to help establish whether the Council is likely to be a long-term borrower or long-term investor in the future, and so shape its strategic focus and decision making. It represents an estimate of the cumulative amount of external borrowing the Council must hold to fund its current capital and revenue plans while keeping treasury investments at the minimum level of £10m required to manage day-to-day cash flow.

	31.3.23 Estimate	31.3.24 Forecast	31.3.25 Forecast	31.3.26 Forecast
Loans CFR	95.2	102.6	104.5	108
Less: Balance sheet resources	-75.9	-63.4	-60.6	-66.5
Net loans requirement	19.3	39.3	44	41.5
Plus: Liquidity allowance	10	10	10	10
Liability benchmark	29.3	49.3	54	51.5
Existing external borrowing	62.6	59.8	58.6	57.3

*The 31.3.23 position is an estimate due to statement of accounts not yet being published

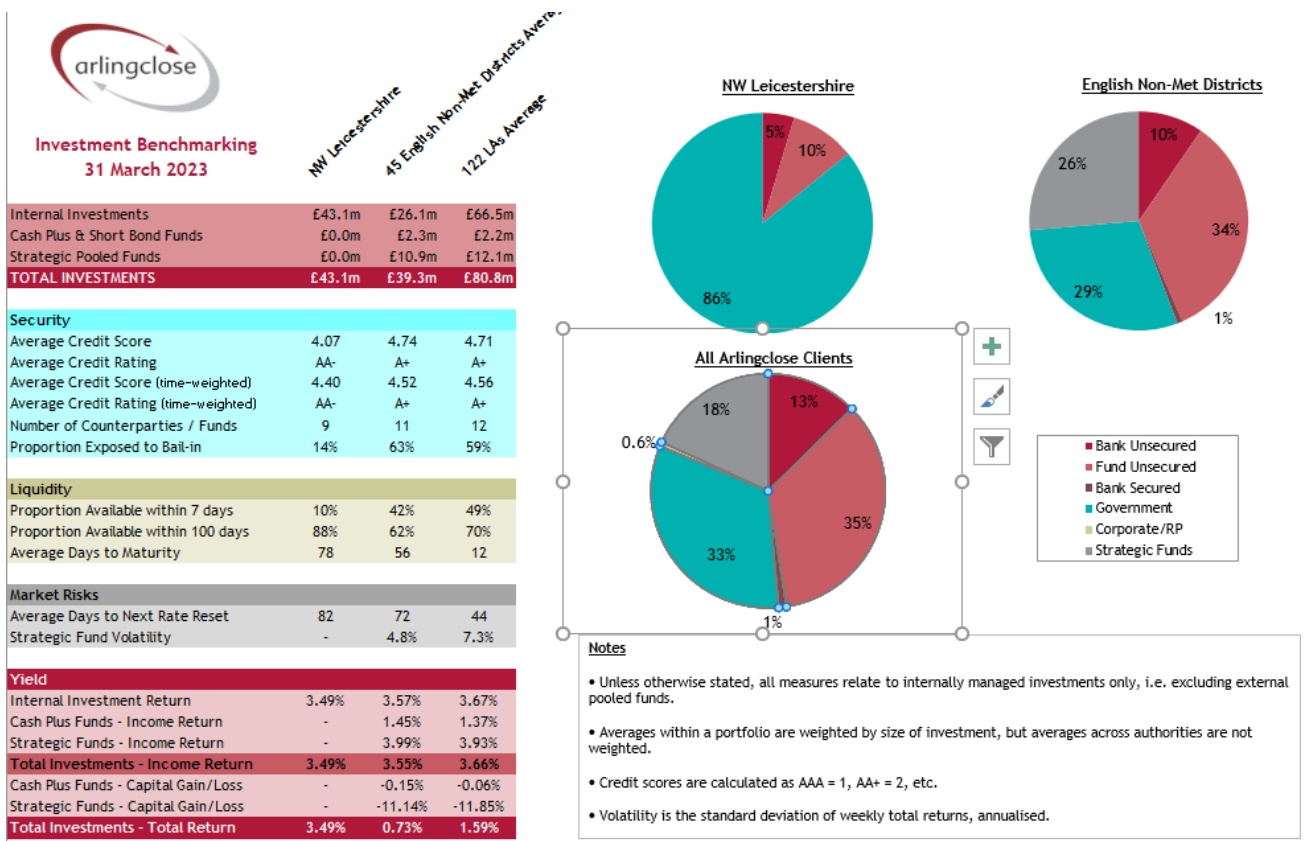
- 10.12 Following on from the medium-term forecast above, the long-term liability benchmark assumes no capital expenditure funded by borrowing after 2023/24, minimum revenue provision on new capital expenditure based on a variable asset life depending on asset type (This can vary from 5 – 50 years) and income, expenditure and reserves all increasing by inflation of 2.5% p.a. This is shown in the chart below together with the maturity profile of the Authority's existing borrowing.

Liability Benchmark - North West Leicestershire



10.13 The Liability Benchmark shows the underlying need to borrow (Loans CFR) in the blue line at the top of the graph, the grey shaded area as existing loans and the strong red line as the requirement for external borrowing. This graph demonstrates that by using internal resources the Council is likely to not have a future external borrowing requirement in addition to borrowing already in place. However, there is little room for adjustment and the Liability Benchmark graph is an estimate and subject to significant change. This situation may evolve and create a borrowing requirement in the next couple of years.

Appendix 1



*Data from last available benchmarking on 31 March 2023

This page is intentionally left blank

NORTH WEST LEICESTERSHIRE DISTRICT COUNCIL

AUDIT AND GOVERNANCE COMMITTEE – WEDNESDAY, 26
JULY 2023

Title of Report	REVIEW OF CORPORATE GOVERNANCE POLICIES	
Presented by	Anna Crouch Head of Finance	
Background Papers	None	Public Report: Yes
Purpose of Report	To receive the committee's comments on the Councils Governance Policies ahead of Cabinet	
Recommendations	THAT THE COMMITTEE PROVIDES ANY COMMENTS IT MAY HAVE FOR CONSIDERATION BY CABINET WHEN IT MEETS TO CONSIDER THE POLICIES ON 19 SEPTEMBER 2023.	

1.0 BACKGROUND

1.1 The Council is responsible for ensuring that its business is conducted in accordance with the law and appropriate standards. In discharging this responsibility, the Council has in place arrangements for governance of its affairs and staff.

1.2 The following documents constitute the Council's suite of Corporate policies:

Policy	Last Reviewed
Anti-Fraud and Corruption Policy	2022
Anti-Money Laundering Policy	2022
Confidential Reporting (Whistleblowing Policy)	2022
Risk Management Policy	2022
RIPA Policy	2022
Information Management Policy	2022
Data Protection Policy	2022
ICT & Cyber Security Policy	2022
Local Code of Corporate Governance	2022

1.3 An annual review of the suite of policies has been undertaken and the revised draft policies are appended to this report. The Committee's views are sought ahead of consideration of the policies at Cabinet in September 2023.

2.0 POLICY REVIEW

2.1 The policies have been reviewed by a team comprising Legal, Internal Audit, ICT, the Monitoring Officer, the Data Protection Officer and the Section 151 Officer.

The main changes to each policy are summarised below:

Anti-Fraud and Corruption Policy

Update to reflect the Council's new management structure and latest terminology within the Council.

Anti-Money Laundering Policy

Updates to reflect the Council's new management structure and latest terminology within the Council.

Confidential Reporting (Whistleblowing Policy)

Update to reflect the Council's new management structure and latest terminology within the Council. Also update reference to the Council's external audit firm.

Risk Management Policy

Update to include a new section on the current challenges facing the Council. This is in response to a recommendation made by Zurich following a recent review of the Council's risk management approach. In addition changes have been made to reflect the Council's new management structure and latest terminology within the Council.

RIPA Policy

Update of Officers that are able to act as "Authorising Officers" under the Regulation of Investigatory Powers Act 2000 (RIPA) to include Heads of Service (previously was just the Chief Executive and the Strategic Directors) – see paragraph 8.6. This change has been made to reflect the change made to the Constitution earlier this year (Part 2, Sec G4, Para 1.5) which includes Heads of Service as Alternative Proper Officers for the purpose of Part 11 of RIPA (Authorised Officers who may authorise, review or cancel the carrying out of directed surveillance or the use of covert human intelligence sources).

Also update to reflect the Council's new management structure and latest terminology within the Council.

Information Management Policy

Update made to reference UK GDPR. Update made to the Data Protection Officer role details and update to the Council's address.

Data Protection Policy

There have been no changes to this Policy.

ICT & Cyber Security Policy

There have been no changes to this Policy.

Local Code of Corporate Governance

Update in relation to the importance of the role of internal audit in the Council's governance and assurance processes.

Policies and other considerations, as appropriate	
Council Priorities:	Our communities are safe, healthy and connected
Policy Considerations:	All those detailed within this report
Safeguarding:	Whistleblowing, surveillance using RIPA and Protecting people's data are all considered to be safeguarding our communities
Equalities/Diversity:	The opportunity for whistleblowing helps to ensure any risk of inequality or lack of diversity can be highlighted.
Customer Impact:	Anti-fraud, anti-money laundering and corruption will protect the customer from financial impact
Economic and Social Impact:	Anti-fraud, anti-money laundering and corruption will protect the customer from economic impact
Environment and Climate Change:	N/A
Consultation/Community/Tenant Engagement:	N/A
Risks:	Risk Management Policy
Officer Contact	Anna Crouch Head of Finance Anna.crouch@nwleicestershire.gov.uk

This page is intentionally left blank

ANTI-FRAUD AND CORRUPTION POLICY

A guide to the Council’s approach to preventing fraud and corruption and managing suspected cases

Version No.	Author	Date	Summary of Changes
2.1	Anna Wright, Senior Auditor	September 2015	
2.2	Lisa Marron, Audit Manager	October 2019	
2.3	Kerry Beavis, Senior Auditor	May 2020	
2.4	Kerry Beavis, Senior Auditor	June 2021	
2.5	Kerry Beavis, Audit Manager	June 2022	
2.6	Kerry Beavis, Audit Manager	June 2023	Minor amendments – name and job title changes.

**Version 2.6
June 2023**

	Contents	Page No.
1.	Introduction	3
2.	Scope	3
3.	Definitions	3
4.	Culture	4
5.	Responsibilities	5
6.	Prevention and deterrence	7
7.	Detection and investigation	9
8.	Raising concerns	10
9.	Review	10
Appendix A		11

ANTI-FRAUD AND CORRUPTION POLICY

1. INTRODUCTION

- 1.1 North West Leicestershire District Council has a duty to ensure that it safeguards the public money that it is responsible for. The Council expects the highest standards of conduct and integrity from all that have dealings with it including staff, members, contractors, volunteers and the public. It is committed to the elimination of fraud and corruption and to ensuring that all activities are conducted ethically, honestly and to the highest standard of openness and accountability so as to protect public safety and public money.
- 1.2 All suspicions or concerns of fraudulent or corrupt practise will be investigated. There will be no distinction made in investigation and action between cases that generate financial benefits and those that do not. Any investigations will not compromise the Council's commitment to Equal Opportunities or the requirements of the Human Rights Act or any other relevant statutory provision.

2. SCOPE

- 2.1 This policy provides an overview of the measures designed to combat any attempted fraudulent or corrupt act, whether attempted internally or externally. The policy is designed to:
- encourage prevention;
 - promote detection;
 - ensure effective investigation where suspected fraud or corruption has occurred;
 - prosecute offenders where appropriate; and
 - recover losses in all instances of fraud or financial irregularity where possible.

3. DEFINITIONS

3.1 Fraud

The Fraud Act 2006 is legislation that has been introduced in order to provide absolute clarity on the subject of fraud. Section 1 of the Act introduced a new general offence of fraud and three ways of committing it:

- fraud by false representation;
- fraud by failing to disclose information; and
- fraud by abuse of position.

Fraud by false representation requires:

- dishonesty;
- an intent to make gain or cause loss; and
- the person makes the representation knowing that it is or might be untrue or misleading.

Fraud by failing to disclose information requires:

- dishonesty;
- an intent to make gain or cause loss; and

- failure to disclose information where there is a legal duty to disclose.

Fraud by abuse of position requires:

- dishonesty;
- an intent to make gain or cause loss; and
- abuse of a position where one is expected to safeguard another person's financial interests.

3.2 Corruption

Corruption is a form of dishonesty or criminal activity undertaken by a person or organisation entrusted with a position of authority, often to acquire illicit benefit.

3.3 Bribery

Broadly the Bribery Act 2010 defines bribery as giving or receiving a financial or other advantage in connection with the "improper performance" of a position of trust, or a function that is expected to be performed impartially or in good faith.

3.4 Money Laundering

Money laundering describes offences involving the integration of the proceeds of crime, or terrorist funds, into the mainstream economy. Whilst the risk of money laundering to the Council is relatively low and the provision of The Money Laundering Regulations 2007 do not strictly apply to the Council, the Council has adopted an Anti-Money Laundering policy as good practice. This policy supports staff in complying with the money laundering provisions included within the Proceeds of Crime Act 2002 and the Terrorism Act 2000.

4. **CULTURE**

- 4.1 We have determined that the culture and tone of the organisation will be one of honesty and opposition to fraud and corruption. We will not tolerate malpractice or wrongdoing in the provision of our services and are prepared to take vigorous action to stamp out any instances of this kind of activity. The fight against fraud and corruption can only be truly effective where these acts are seen as anti-social unacceptable behaviour and whistle blowing is perceived as a public-spirited action.
- 4.2 The prevention/detection of fraud/corruption and the protection of public money are responsibilities of everyone, both internal and external to the organisation. The Council's elected members and employees play an important role in creating and maintaining this culture. They are positively encouraged to raise concerns regarding fraud and corruption, immaterial of seniority, rank or status, in the knowledge that such concerns will wherever possible be treated in confidence. The public also has a role to play in this process and should inform the Council if they feel that fraud/corruption may have occurred. The Nolan Committee on Standards in Public Life set out the seven guiding principles (Appendix A) that apply to people who serve the public.
- 4.3 Concerns must be raised when members, employees or the public reasonably believe that one or more of the following has occurred or is in the process of occurring or is likely to occur:
- a criminal offence;
 - a failure to comply with a statutory or legal obligation;
 - improper or unauthorised use of public or other official funds;
 - a miscarriage of justice;
 - maladministration, misconduct or malpractice;

- endangering an individual's health and/or safety;
 - damage to the environment; and
 - deliberate concealment of any of the above.
- 4.4 The Council will ensure that any allegations received in any way, including by anonymous letter or telephone call, will be taken seriously and investigated in an appropriate manner. The Council has a [Confidential Report \(Whistleblowing\) policy](#) that sets out the approach to these types of allegation in more detail.
- 4.5 The Council will take action against those who defraud the Council or who are corrupt or where there has been financial malpractice. There is, of course, a need to ensure that any investigation process is not misused and, therefore, any abuse (such as employees raising malicious allegations) may be dealt with as a disciplinary matter.
- 4.6 Where fraud or corruption has occurred due to a breakdown in the Council's systems or procedures, the Head of Service will ensure that appropriate improvements in systems of control are implemented in order to prevent re- occurrence.

5. RESPONSIBILITIES

5.1 Responsibilities of Elected Members

As elected representatives, all members of the Council have a duty to protect the Council and public money from any acts of fraud and corruption. This is done through existing practice, compliance with the Members' Code of Conduct, the Council's Constitution including Financial Regulations and Standing Orders and relevant legislation.

5.2 Responsibilities of the Monitoring Officer

The Monitoring Officer is responsible for ensuring that all decisions made by the Council are within the law. The Monitoring Officer's key role is to promote and maintain high standards of conduct throughout the Council by developing, enforcing and reporting appropriate governance arrangements including codes of conduct and other standards policies.

5.3 Responsibilities of the Section 151 Officer

The Director of Resources has been designated as the statutory officer responsible for financial matters as defined by s151 of the Local Government Act 1972. The legislation requires that every local authority in England and Wales should 'make arrangements for the proper administration of their financial affairs and shall secure that one of their officers has the responsibility for the administration of those affairs'.

Under the Director of Resources responsibilities, 'proper administration' encompasses all aspects of local authority financial management including:

- compliance with the statutory requirements for accounting and internal audit;
- managing the financial affairs of the Council;
- the proper exercise of a wide range of delegated powers both formal and informal;
- the recognition of the fiduciary responsibility owed to local tax payers.

Under these statutory responsibilities the Section 151 Officer contributes to the antifraud and corruption framework of the Council.

5.4 Responsibilities of Employees

Each employee is governed in their work by the Council's Standing Orders and Financial Regulations, and other codes on conduct and policies (Employee Code of Conduct, Health and Safety Policy, ICT and Cyber Security Policy). Included in the Employee Code of Conduct are guidelines on Gifts and Hospitality, and advice on professional and personal conduct and conflicts of interest. These are issued to all employees when they join the Council. Appropriate disciplinary procedures will be invoked where there is a breach of policy.

Employees are responsible for ensuring that they follow instructions given to them by management, particularly in relation to the safekeeping of the assets of the Council.

Employees are expected always to be aware of the possibility that fraud, corruption and theft may exist in the workplace and be able to share their concerns with management.

5.5 Role of the Leicestershire Revenues and Benefits Partnership Fraud Investigation Team

The Fraud Team based at the Leicestershire Revenues and Benefits Partnership are responsible for the investigation of all revenues and benefit related alleged/suspected fraud cases. Due to the specialised nature of these investigations, a separate sanctions policy has been developed that covers all aspects of the investigation process.

5.6 Role of the External Auditors

Independent external audit is an essential safeguard of the stewardship of public money. This is currently carried out by Azets through specific reviews that are designed to test (amongst other things) the adequacy of the Council's financial systems and arrangements for preventing and detecting fraud and corruption. It is not the external auditor's function to prevent fraud and irregularities, but the integrity of public funds is at all times a matter of general concern. External auditors are always alert to the possibility of fraud and irregularity and will act without undue delay if grounds for suspicion come to their notice.

5.7 Role of the Public

This policy, although primarily aimed at those within or associated with the Council, enables concerns raised by the public to be investigated, as appropriate, by the relevant person in a proper manner.

5.8 Conflicts of Interest

Both elected members and employees must ensure that they avoid situations where there is a potential for a conflict of interest. Such situations can arise with externalisation of services, internal tendering, planning and land issues etc. Effective role separation will ensure decisions made are seen to be based on impartial advice and avoid questions about improper disclosure of confidential information.

6. PREVENTION AND DETERRENCE

6.1 Responsibilities of the Senior Management Team

Managers at all levels are responsible for the communication and implementation of this policy. They are also responsible for ensuring that their employees are aware of the Council's policies and procedures relating to financial management and conduct and that the requirements are being met. Managers are expected to create an environment in which their staff feel able to approach them with any concerns they may have about suspected irregularities. Special arrangements may be applied from time to time for example where employees are responsible for cash handling or are in charge of financial systems and systems that generate payments, for example payroll or the Council Tax system. These procedures should be supported by relevant training.

Management has responsibility for the prevention of fraud and corruption within all departments. It is essential that managers understand the importance of soundly designed systems which meet key control objectives and minimise opportunities for fraud and corruption. They are responsible for assessing the potential for fraud and corruption within their own department's activities and for implementing appropriate strategies to minimise this risk.

The Council recognises that a key preventative measure in dealing with fraud and corruption is for managers to take effective steps at recruitment stage to establish, as far as possible, the honesty and integrity of potential employees, whether for permanent, temporary or casual posts and agency staff. The Council's formal recruitment procedures contain appropriate safeguards in the form of written references, the verification of qualifications held and employment history. Disclosure and Barring Service (DBS) checks are undertaken for employees working with or who may have contact with children and vulnerable adults.

6.2 Role of Internal Audit

Internal Audit plays a preventative role in trying to ensure that systems and procedures are in place to prevent and deter fraud and corruption. Internal Audit may be requested to investigate cases of suspected financial irregularity, fraud or corruption, except Benefit fraud investigations and Single Person Discount fraud, in accordance with agreed procedures. Within the Financial Procedures Rules in the Constitution, representatives of Internal Audit have the authority to:

- enter any Council owned or occupied premises or land at all times (subject to any legal restrictions outside the Council's control);
- have access at all times to the Council's records, documents and correspondence;
- require and receive such explanations from any employee or member of the Council as he or she deem necessary concerning any matter under examination; and
- require any employee or member of the Council to produce cash, stores or any other Council owned property under their control.

Internal Audit liaises with management to recommend changes in procedures to reduce risks and prevent losses to the Authority.

6.3 Working with Others and Sharing Information

The Council is committed to working and co-operating with other organisations to prevent fraud and corruption and protect public funds. The Council may use personal

information and data-matching techniques to detect and prevent fraud, and ensure public money is targeted and spent in the most appropriate and cost-effective way. In order to achieve this, information may be shared with other bodies for auditing or administering public funds including the Cabinet Office, the Department of Work and Pensions, other local authorities, National Anti-Fraud Network, HM Revenues and Customs, and the Police.

6.4 National Fraud Initiative (NFI)

The Council participates in the National Fraud Initiative (NFI). This requires public bodies to submit a number of data sets, for example payroll, Council Tax, and accounts payable (but not limited to these) which is then matched to data held by other public bodies. Any positive matches (e.g. an employee on the payroll in receipt of housing benefit) are investigated.

6.5 Data Sharing

In the interests of protecting the public purse and the prevention and detection of fraud, members of staff are actively encouraged to report any instances of fraud. We have published fair processing notices on our website and also display this information in our public areas, notifying members of the public that we will share information held between departments and other third party organisations as appropriate in order to prevent and detect crime.

6.6 Training and Awareness

The successful prevention of fraud is dependent on risk awareness, the effectiveness of training and the responsiveness of staff throughout the Council. The Council recognises that the continuing success of this policy and its general credibility will depend in part on the effectiveness of training and awareness for members and employees and will therefore take appropriate action to raise awareness levels.

6.7 Disciplinary Action

The Council's Disciplinary Procedures will be used to facilitate a thorough investigation of any allegations of improper behaviour by employees. Theft, fraud and corruption are serious offences which may constitute gross misconduct against the Council and employees will face disciplinary action if there is evidence that they have been involved in these activities, including benefit fraud. Disciplinary action will be taken in addition to, or instead of, criminal proceedings depending on the circumstances of each individual case.

Members will face appropriate action under this policy if they are found to have been involved in theft, fraud or corruption against the Authority. Action will be taken in addition to, or instead of criminal proceedings, depending on the circumstances of each individual case but in a consistent manner. If the matter is a breach of the Members' Code of Conduct then it will be dealt with under the arrangements agreed by the Council in accordance with the Localism Act 2011.

6.8 Prosecution

In terms of proceedings the Council will endeavour to take action in relevant cases to deter others from committing offences against the Authority. Any prosecution will be in accordance with the principles contained within The Code for Crown Prosecutors.

6.9 Publicity

The Council will optimise the publicity opportunities associated with anti-fraud and corruption activity within the Council. Wherever possible, where the Council has suffered a financial loss action will be taken to pursue the recovery of the loss.

All anti-fraud and corruption activities, including the update of this policy, will be publicised in order to make employees and the public aware of the Council's commitment to taking action on fraud and corruption when it occurs.

7. **DETECTION AND INVESTIGATION**

7.1 Although audits may detect fraud and corruption as a result of the work that they are undertaking, the responsibility of the detection of financial irregularities primarily rests with management. Included within the audit plans are reviews of system controls including financial controls and specific fraud and corruption tests, spot checks and unannounced visits.

In addition to Internal Audit, there are numerous systems and management controls in place to deter fraud and corruption but it is often the vigilance of employees and members of the public that aids detection. In some cases frauds are discovered by chance or 'tip-off' and the Council will ensure that such information is properly dealt with within its Confidential Reporting (Whistleblowing) policy.

The Council is committed to the investigation of all instances of actual, attempted and suspected fraud committed by employees, members, consultants, suppliers and other third parties and the recovery of funds and assets lost through fraud.

Any suspected fraud, corruption or other irregularity should be reported to Internal Audit. The Audit Manager will decide on the appropriate course of action to ensure that any investigation is carried out in accordance with Council policies and procedures, key investigation legislation and best practice. This will ensure that investigations do not jeopardise any potential disciplinary action or criminal sanctions.

Action could include:

- investigation carried out by Internal Audit staff;
- joint investigation with Internal Audit and relevant directorate management;
- directorate staff carry out investigation and Internal Audit provide advice and guidance;
- referral to the Police.

The responsibility for investigating potential fraud, corruption and other financial irregularities within the Council lies mainly (although not exclusively) with the Internal Audit section.

8. RAISING CONCERNS

8.1 All suspected or apparent fraud or financial irregularities must be raised, in the first instance, directly with the manager or if necessary in accordance with the Council's [Confidential Reporting \(Whistleblowing\) Policy](#). Advice and guidance on how to pursue matters of concern may be obtained from the Council's nominated contact points who are:

- Chief Executive: Allison.thomas@nwleicestershire.gov.uk
Telephone 01530 454500
- Monitoring Officer: elizabeth.warhurst@nwleicestershire.gov.uk
Telephone 01530 454762
- Section 151 Officer: glenn.hammons@nwleicestershire.gov.uk
- Audit Manager: kerry.beavis@nwleicestershire.gov.uk
Telephone 01530 454728

9. Review

9.1 This policy will be reviewed annually or if legislation changes sooner.

APPENDIX A

THE SEVEN PRINCIPLES OF PUBLIC LIFE

Selflessness

Holders of public office should take decisions solely in terms of the public interest. They should not do so in order to gain financial or other material benefits for themselves, their family, or their friends.

Integrity

Holders of public office should not place themselves under any financial or other obligation to outside individuals or organisation that might influence them in the performance of their official duties.

Objectivity

In carrying out public business, including making public appointments, awarding contracts or recommending individuals for rewards and benefits, holders of public office should make choices on merit.

Accountability

Holders of public office are accountable for their decisions and actions to the public and must submit themselves to whatever scrutiny is appropriate to their office.

Openness

Holders of public office should be as open as possible about all the decisions and action that they take. They should give reasons for their decisions and restrict information only when the wider public interest clearly demands.

Honesty

Holders of public office have a duty to declare any private interests relating to their public duties and to take steps to resolve any conflicts arising in a way that protects the public interest.

Leadership

Holders of public office should promote and support these principles by leadership and example.

Committee on Standards in Public Life - The Nolan Report (1995)

This page is intentionally left blank

ANTI-MONEY LAUNDERING POLICY

A guide to the Council's anti-money laundering safeguards and reporting arrangements

Version No.	Author	Date	Summary of Changes
2.1	Anna Wright, Senior Manager	September 2015	
2.2	Kerry Beavis, Senior Auditor	May 2020	
2.3	Kerry Beavis, Senior Auditor	June 2021	
2.4	Kerry Beavis, Audit Manager	June 2022	
2.5	Kerry Beavis, Audit Manager	June 2023	Minor amendments of name changes.

**Version 2.5
June 2023**

	Contents	Page No.
1.	Introduction	3
2.	Scope of the policy	3
3.	Definition of money laundering	3
4.	Requirements of the money laundering legislation	4
5.	The money laundering reporting officer (MLRO)	4
6.	Client identification procedures	5
7.	Reporting procedure for suspicions of money laundering	5
8.	Consideration of the disclosure by the money laundering reporting officer	6
9.	Training	7
10.	Review	7

ANTI-MONEY LAUNDERING POLICY

1. INTRODUCTION

- 1.1 The Council is committed to the highest possible standards of conduct and has, therefore, put in place appropriate and proportionate anti-money laundering safeguards and reporting arrangements. Although local authorities are not directly covered by the requirements of the Money Laundering and Terrorist Financing (Amendment) Regulations 2019, they are bound by the Proceeds of Crime Act 2002 and the Terrorism Act 2006, both of which place a number of duties and responsibilities on local authorities and employees and members of the same, in order that they do not find themselves subject to criminal prosecution.

2. SCOPE OF THE POLICY

- 2.1 This policy applies to all employees, whether permanent or temporary, and members of the Council. Its aim is to enable employees and members to respond to a concern they have in the course of their dealings for the Council. Individuals who may have a concern relating to a matter outside work should contact the Police.

3. DEFINITION OF MONEY LAUNDERING

- 3.1 Money laundering is a term designed to cover a number of offences. These offences relate to the improper handling of funds that are the proceeds of criminal acts, or terrorist acts, so that they appear to come from a legitimate source. It relates to both the activities of organised crime but also to those who benefit financially from dishonest activities such as receiving stolen goods. The Proceeds of Crime Act 2002 (POCA), as amended by the Serious Organised Crime and Police Act 2005, creates a range of criminal offences arising from dealing with proceeds of crime.

The four main offences that may be committed under money laundering legislation are:

- concealing, disguising, converting, transferring or removing criminal property from anywhere in the UK;
- entering into or becoming concerned in an arrangement which a person knows, or suspects facilitates, the acquisition, retention, use or control of criminal property by or on behalf of another person;
- acquiring, using or possessing criminal property*;
- entering into or being concerned in an arrangement which facilitates the retention or control by or on behalf of another person of terrorist property ** by concealment, removal, transfer or in any other way.

It is also an offence to attempt, conspire or incite to commit any of the above offences and to aid, abet, counsel, or procure the commission of any of the above offences.

* Criminal property is something which constitutes a person's benefit from criminal conduct or represents such benefit; it is not limited to money and there is no minimum amount.

** Terrorist property includes money or other property likely to be used for terrorism, proceeds of terrorist acts, and proceeds of acts carried out for the purposes of terrorism.

There are also two 'third party' offences:

- failing to disclose information relating to money laundering offences (in respect of both criminal property and terrorist property) where there is reasonable grounds for knowledge or suspicion ***; and,
- tipping off or informing someone who is, or is suspected of, being involved in money laundering activities, in such a way as to reduce the likelihood of or prejudice an investigation.

*** It is important to note that whilst the disclosure obligations and tipping off offences in relation to criminal property will not always strictly apply to local authorities all individuals and businesses have an obligation to report knowledge, reasonable grounds for belief or suspicion about the proceeds from terrorism, proceeds of acts carried out for the purposes of terrorism or likely to be used for terrorism, where that information has come to them in the course of their business or employment.

3.2 The Terrorism Act made it an offence of money laundering to become concerned in an arrangement relating to the retention or control of property likely to be used for the purpose of terrorism or resulting from acts of terrorism.

3.3 Although the term 'money laundering' is generally used to describe the activities of organised crime for most people it will involve a suspicion that someone they know, or know of, is benefiting financially from dishonest activities.

3.4 Potentially very heavy penalties (unlimited fines and imprisonment up to fourteen years) can be handed down to those who are convicted of one of the offences above.

4. REQUIREMENTS OF THE MONEY LAUNDERING LEGISLATION

4.1 The main requirements of the legislation are:

- to appoint a money laundering reporting officer;
- maintain client identification procedures in certain circumstances;
- implement a procedure to enable the reporting of suspicions of money laundering;
- maintain record keeping procedures.

5. THE MONEY LAUNDERING REPORTING OFFICER (MLRO)

5.1 The Council has designated the Section 151 Officer as the Money Laundering Reporting Officer (MLRO). He can be contacted at glenn.hammons@nwleicestershire.gov.uk.

In the absence of the MLRO or instances where it is suspected that the MLRO themselves are involved in suspicious transactions, concerns should be raised with the Deputy Section 151 Officer, who can be contacted on 01530 454492 or at anna.crouch@nwleicestershire.gov.uk.

6. CLIENT IDENTIFICATION PROCEDURES

- 6.1 Although not a legal requirement, the Council has developed formal client identification procedures which must be followed when Council land or property is being sold. These procedures require individuals and, if appropriate, companies to provide proof of identity and current address.

If satisfactory evidence is not obtained at the outset of a matter, then the transaction must not be progressed and a disclosure report, available on the intranet, must be submitted to the Money Laundering Reporting Officer.

All personal data collected must be kept in compliance with the Data Protection Act 2018.

7. REPORTING PROCEDURE FOR SUSPICIONS OF MONEY LAUNDERING

- 7.1 Where you know or suspect that money laundering activity is taking/has taken place or become concerned that your involvement in a matter may amount to a prohibited act under the Act, you must disclose this as soon as practicable to the MLRO. The disclosure should be within 'hours' of the information coming to your attention, not weeks or months.
- 7.2 Your disclosure should be made to the MLRO using the disclosure form, available on the intranet.

The report must include as much detail as possible including:

- full details of the person involved;
- full details of the nature of their/your involvement;
- the types of money laundering activity involved;
- the dates of such activities;
- whether the transactions have happened, are ongoing or are imminent;
- where they took place;
- how they are undertaken;
- the (likely) amount of money/assets involved; and
- why, exactly, you are suspicious.

Along with any other available information to enable the MLRO to make a sound judgement as to whether there are reasonable grounds for knowledge or suspicion of money laundering and to enable them to prepare their report to the National Crime Agency (NCA), where appropriate. You should also enclose copies of any relevant supporting documentation.

- 7.3 If you are concerned that your involvement in the transaction would amount to a prohibited act under sections 327-329 of the Proceeds of Crime Act 2002, then your report must include all relevant details, as you will need consent from the NCA, via the MLRO, to take any further part in the transaction – this is the case even if the client gives instructions for the matter to proceed before such consent is given. You should therefore make it clear in the report if such consent is required and clarify whether there are any deadlines for giving such consent e.g. a completion date or court deadline.

- 7.4 Once you have reported the matter to the MLRO you must follow any directions they may give you. You must NOT make any further enquiries into the matter yourself, any necessary investigation will be undertaken by the NCA. Simply report your suspicions to the MLRO who will refer the matter on to the NCA if appropriate. All members of staff will be required to co-operate with the MLRO and the authorities during any subsequent money laundering investigation.
- 7.5 Similarly, at no time and under no circumstances should you voice any suspicions to the person(s) whom you suspect of money laundering, even if the NCA has given consent to a particular transaction proceeding, without the specific consent of the MLRO; otherwise, you may commit a criminal offence of 'tipping off'.
- 7.6 Do not, therefore, make any reference on a client file, to a report having been made to the MLRO - should the client exercise their right to see the file, then such a note will obviously tip them off to the report having been made and may render you liable to prosecution. The MLRO will keep the appropriate records in a confidential manner.

8. CONSIDERATION OF THE DISCLOSURE BY THE MONEY LAUNDERING REPORTING OFFICER

- 8.1 Upon receipt of a disclosure report, the MLRO must note the date of receipt on their section of the report and acknowledge receipt of it. They should also advise you of the timescale within which they expect to respond to you.
- 8.2 The MLRO will consider the report and any other available internal information they think is relevant, e.g.
- reviewing other transaction patterns and volumes;
 - the length of any business relationship involved;
 - the number of any one-off transactions and linked one-off transactions;
 - any identification evidence held;

and undertake such other reasonable enquiries they think appropriate in order to ensure that all available information is taken into account in deciding whether a report to the NCA is required (such enquiries being made in such a way as to avoid any appearance of tipping of those involved). The MLRO may also need to discuss the report with you.

- 8.3 Once the MLRO has evaluated the disclosure report and any other relevant information, they must make a timely determination as to whether:
- there is an actual or suspected money laundering taking place; or
 - whether there are reasonable grounds to know or suspect that this is the case; and
 - whether they need to seek consent from the NCA for a particular transaction to proceed.
- 8.4 Where the MLRO does so conclude, then they must disclose the matter as soon as practicable to the NCA on their standard report form and in the prescribed manner, unless they have a reasonable excuse of non-disclosure to the NCA (for example, if you are a lawyer and you wish to claim legal professional privilege for not disclosing the information).

- 8.5 Where the MLRO suspects money laundering but has a reasonable excuse for nondisclosure, then they must note the report accordingly, they can then immediately give their consent for any ongoing or imminent transactions to proceed. In cases where legal professional privilege may apply, the MLRO must liaise with the Council's Monitoring Officer to decide whether there is a reasonable excuse for not reporting the matter to the NCA.
- 8.6 Where consent is required from the NCA for a transaction to proceed, then the transaction(s) in question, must not be undertaken or completed until the NCA has given specific consent, or there is deemed consent through the expiration of the relevant time limits in which the NCA must respond, and no response has been received.
- 8.7 Where the MLRO concludes that there are no reasonable grounds to suspect money laundering then they shall mark the report accordingly and give their consent for any ongoing or imminent transaction(s) to proceed.
- 8.8 All disclosure reports referred to the MLRO and reports made by them to the NCA must be retained by the MLRO in a confidential file kept for that purpose, for a minimum of five years.
- 8.9 The MLRO commits a criminal offence if they know or suspect, or have reasonable grounds to do so, through a disclosure being made to them, that another person is engaged in money laundering and does not disclose this as soon as practicable to the NCA.

9. TRAINING

- 9.1 Officers considered likely to be exposed to suspicious situations, will be made aware of these by their senior officer and provided with appropriate training.
- 9.2 Additionally, all employees and members will be familiarised with the legal and regulatory requirements relating to money laundering and how they affect both the Council and themselves.
- 9.3 Notwithstanding the paragraphs above, it is duty of officers and members to report all suspicious transactions whether they have received their training or not.

10. REVIEW

- 10.1 This policy will be reviewed annually and whenever the relevant legislation changes.

This page is intentionally left blank

CONFIDENTIAL REPORTING (WHISTLEBLOWING) POLICY

Version No.	Author	Date	Summary of Changes
2.1	Kerry Beavis, Senior Auditor	May 2020	
2.2	Kerry Beavis, Senior Auditor	June 2021	
2.3	Kerry Beavis, Audit Manager	June 2022	
2.4	Kerry Beavis, Audit Manager	June 2023	Minor amendments, including name changes and update to external audit firm.

Version 2.4
June 2023

	Contents	Page No.
1.	Introduction	3
2.	Aims and scope of policy	4
3.	Safeguards – Harassment or Victimisation	4
4.	Confidentiality	5
5.	Anonymous allegations	6
6.	Untrue allegations	6
7.	How to raise a concern	6
8.	How the council will respond	7
9.	The Responsible Officer	8
10.	How the matter can be taken further	9
11.	Review	9

CONFIDENTIAL REPORTING (WHISTLEBLOWING) POLICY

“North West Leicestershire District Council is committed to the prevention, deterrence, detection and investigation of fraud, corruption, and malpractice in all forms. It encourages employees and members of the Council and its contractors who have serious concerns about any aspect of its work, including matters of health and safety, to voice those concerns.”

1. INTRODUCTION

1.1 The Council is committed to the highest possible standards of openness, probity and accountability. In line with that commitment, we expect employees, members and others that we deal with, who have serious concerns about any aspect of the Council's work to come forward and voice those concerns. This Confidential Reporting Policy is intended to encourage and enable employees, members, contractors, or suppliers to raise serious concerns **within** the Council rather than overlooking a problem or “blowing the whistle” outside.

1.2 This Policy provides guidance on the way in which concerns may be raised.

This Policy also sets out how matters can be taken further if a person remains dissatisfied with the Council's response to any concerns raised.

1.3 Employees, members, contractors, and suppliers are often the first to realise that there may be something seriously wrong within the Council. However, they may not express their concerns because they feel that speaking up would be disloyal to their colleagues or to the Council, or they perceive that it could harm their chances of future business or their career prospects. They may also fear harassment or victimisation. In such circumstances individuals may consider it to be easier to ignore the concern rather than report what may only be a suspicion of malpractice. This Policy document makes it clear that individuals raising concerns will do so without fear of victimisation, subsequent discrimination, or disadvantage.

1.4 It is recognised that, where concerns are raised, most cases will have to proceed on a confidential basis. The Council will do everything it can to protect the confidentiality of those individuals raising concerns. However, there may be times when the person making the complaint can be identified due to the nature of the allegation made and, in such cases, it will not be possible to keep the identity of the complainant confidential. In addition, there may be times when the Council will believe it is appropriate to let the subject of a complaint know who made any allegation.

1.5 The Council recognises that individuals raising concerns, termed “qualifying disclosures” under the Public Interest Disclosure Act 1998 are entitled to protection under that Act and/or this Policy and may be eligible to compensation if they subsequently suffer victimisation, discrimination, or disadvantage. Under the Enterprise and Regulatory Reform Act 2013, any disclosure using the Whistleblowing Policy, within reasonable belief of the worker making the disclosure will only be protected if it is made in the public interest. It must also show one or more of the following:

- (a) that a criminal offence has been committed, is being committed or is likely to be committed,
- (b) that a person has failed, is failing or is likely to fail to comply with any legal obligation to which he is subject,
- (c) that a miscarriage of justice has occurred, is occurring or is likely to occur,

- (d) that the health or safety of any individual has been, is being or is likely to be endangered,
- (e) that the environment has been, is being or is likely to be damaged, or
- (f) that information tending to show any matter falling within any one of the preceding paragraphs has been, is being or is likely to be deliberately concealed.

1.6 This policy is designed for workers. Workers include:

- Employees;
- Agency workers;
- People that are training with an employer;
- Self-employed workers, if supervised or working on site.

1.7 The procedures outlined in this Policy **are in addition to** the Council's complaints procedures and other statutory reporting procedures applying to some divisions.

1.8 This Policy has been discussed with the relevant trade unions and has their support.

1.9 The principles of this Policy also apply to concerns of the general public.

2. AIMS AND SCOPE OF THE POLICY

2.1 This Policy aims to:

- encourage you to feel confident in raising concerns that are in the public interest and to question and act upon your concerns;
- provide avenues for you to raise those concerns and receive feedback on any action taken;
- ensure that you receive a response to your concerns and that you are aware of how to pursue matters if you are not satisfied;
- reassure you that you will be protected from the risk of reprisals or victimisation if you have a reasonable belief that you have made any disclosure in good faith.

2.2 If Council employees have concerns relating to their employment with the organisation, these should be raised under the Council's Grievance Policy. This Policy is intended to cover major concerns that fall outside the scope of other policies and procedures. As stated in paragraph 1.5, these include:

- conduct which is an offence or a breach of law,
- disclosures related to miscarriages of justice,
- health and safety risks, including risks to the public as well as other employees,
- damage to the environment,
- the unauthorised use of public funds,
- possible fraud and corruption,
- sexual or physical abuse of clients, or
- other unethical conduct.

3. SAFEGUARDS - HARASSMENT OR VICTIMISATION

3.1 The Council is committed to good practice and high standards and aims to be

supportive of employees and others using this policy.

3.2 The Council recognises that the decision to report a concern can be a difficult one to make. You are legally entitled to protection from unfair treatment if:

- (a) you honestly think what you are reporting is true,
- (b) you believe that you are telling the right person,
- (c) you believe that raising your concerns is in the public interest.

Put simply, if you are acting in good faith when raising any concerns, you should have nothing to fear because you will be doing your duty to your employer, and/or the Council and those for whom the Council provides a service. In the event that the concerns raised are substantiated, you will be ensuring that bad practice / unethical behaviour / illegal conduct is curtailed.

3.3 The Council will not tolerate any harassment or victimisation (including informal pressures) against individuals who raise concerns in good faith under this Policy and will take appropriate action to protect those who raise a concern in good faith and, where necessary, will take action against those subjecting any complainant to harassment, victimisation or any other pressures as a result of raising concerns.

3.4 Any investigation into allegations of matters listed in paragraph 2.2 of this Policy will not influence, or be influenced by, any disciplinary, redundancy or similar procedures which may already affect either the person raising the concerns or the individual(s) who are the subject of those concerns.

4. CONFIDENTIALITY

4.1 All attempts will be made to ensure any concerns raised will be treated in confidence and to protect your identity if you so wish. The Council cannot ensure your confidentiality if you have informed others of any alleged concerns.

4.2 In addition, there may be times when the identity of the person making the complaint is clear due to the nature of any allegations made. In such cases, the Council cannot take any steps to protect your identity. You will, however, still be entitled to the same protection against harassment, victimisation, and other pressures as if your identity remained confidential.

4.3 In a small number of cases, the Council may find it is appropriate to disclose your identity to the person who is the subject of any complaint. It will, however, inform you of this before doing so. Again, you will receive the same protection against harassment, victimisation, and other pressures as if your identity had remained confidential.

4.4 You should note that, whilst every effort will be made to protect your identity, the Council may, at an appropriate time ask you to come forward as a witness. If you do become a witness in any case, you will be entitled to the same protection against harassment, victimisation, and other pressures that you are entitled to when making the initial complaint under this Policy.

5. ANONYMOUS ALLEGATIONS

- 5.1 This Policy aims to protect those raising concerns and, therefore, it is hoped that any person raising concerns will do so in their own name whenever possible.
- 5.2 Whilst any concern will be taken seriously, those expressed anonymously will carry less weight but will be given consideration by the Council; an investigation into the matters raised will be investigated at the discretion of the Council.
- 5.3 In exercising this discretion, the factors to be taken into account will include:
- the nature and seriousness of the issues raised,
 - the apparent credibility of the concern, and
 - the probable likelihood of being able to confirm the allegation from attributable sources.
- 5.4 If the Council does not know who has made an allegation, it will not be possible for the Council to offer reassurance and protection to the individual.

6. UNTRUE ALLEGATIONS

- 6.1 If an allegation is made in good faith but is not confirmed following an investigation by the Council, no action will be taken against the person making the allegation. This should encourage those who have concerns to raise it in the appropriate manner without fear of any reprisals.
- 6.2 If, however, an allegation is made frivolously, maliciously or for personal gain, disciplinary action may be taken against the person making that allegation where appropriate.

7. HOW TO RAISE A CONCERN

- 7.1 Advice and guidance on how to pursue matters of concern may be obtained from the Council's nominated contact points who are:
- Chief Executive: Allison.thomas@nwleicestershire.gov.uk
Telephone 01530454500
 - Monitoring Officer: elizabeth.warhurst@nwleicestershire.gov.uk
Telephone 01530 454762
 - Interim Section 151 Officer: glenn.hammons@nwleicestershire.gov.uk
 - Audit Manager: kerry.beavis@nwleicestershire.gov.uk
Telephone 01530 454378
- 7.2 Concerns may be raised verbally or in writing, to any of the above-named individuals. If raising a concern in writing, it should be addressed to the named individual at the:

Council Offices
North West Leicestershire District Council
Whitwick Road
Coalville
Leicestershire
LE67 3FJ

Clearly mark the envelope “Confidential”.

Alternatively you can contact North West Leicestershire District Council’s external auditor at - Azets, 6th Floor, Bank House, Cherry Street, Birmingham, B2 5AL or via email - Gary.Devlin@azets.co.uk

If you wish to make a written report you are invited to use the following format:

- the background and history of the concern (giving relevant dates);
- the reason why you are particularly concerned about the situation.

- 7.3 If you wish to make a verbal report of any concerns that you have identified, you are invited to contact one of the officers named at paragraph 7.1 above to arrange a mutually convenient appointment. When arranging an appointment, it would be helpful if you could mention that you would like to speak to them about a matter under the Confidential Reporting Policy.
- 7.4 When making a verbal report, you are invited to set out the facts using the same format identified at paragraph 7.2 above.
- 7.5 The earlier you express any concerns the easier it is for the Council to investigate and take any relevant action.
- 7.6 Although you are not expected to prove beyond doubt the truth of an allegation, you will need to demonstrate to the person contacted that there are reasonable grounds for your concern.
- 7.7 You may wish to consider discussing your concern with a colleague or trade union representative first and you may find it easier to raise the matter if there are two (or more) of you who share any concerns.
- 7.8 You may invite your trade union, professional association representative or a member of staff to be present during any meetings or interviews in connection with the concerns you have raised.
- 7.9 If you feel unable to raise your concerns directly with the Council, you should report the matter to a “prescribed person”. This will ensure that your legal rights are protected. The list of prescribed persons can change and so up to date information can be obtained by accessing an online brochure entitled “Whistleblowing: list of prescribed people and bodies” available at www.gov.uk

8. HOW THE COUNCIL WILL RESPOND

- 8.1 The Council will respond to your concerns but within the constraints of maintaining confidentiality or observing any legal restrictions. In any event, a confidential record of the steps taken will be kept in accordance with the Data Protection Act 2018.
- 8.2 The Council may also ask to meet with you in order to gain further information from you. Do not forget that testing out your concerns is not the same as either accepting or rejecting them. It is sometimes necessary to test out any concerns raised in order to identify how strong any evidence may be.

8.3 Where appropriate, the matters raised may be:

- investigated internally,
- referred to the police,
- referred to the external auditor,
- made the subject of an independent enquiry.

Following any of the action above, a concern may be upheld or may be dismissed.

8.4 In order to protect individuals and those accused of misdeeds or possible malpractice, the Council will undertake initial enquiries to decide whether an investigation is appropriate and, if so, what form it should take. In most cases, it is anticipated that these initial enquiries will be completed within ten working days of an allegation being made. The overriding principle which the Council will have in mind when deciding what steps to take is whether the matter falls within the public interest. Any concerns or allegations which fall within the scope of any other specific procedures (for example, misconduct or discrimination issues) will normally be referred to the relevant service area for consideration under those procedures.

8.5 Some concerns may be resolved by agreed action without the need for investigation. If urgent action is required this will be taken before any investigation is conducted.

8.6 Within seven working days of a concern being raised, the nominated contact will write to you:

- acknowledging that the concern has been received,
- indicating how we propose to deal with the matter,
- giving an estimate of how long it will take to provide a final response,
- telling you whether any initial enquiries have been made,
- supplying you with information on staff support mechanisms, and
- telling you whether further investigations will take place and if not, why not.

8.7 The amount of contact between the officers considering the issues and you will depend on the nature of the matters raised, the potential difficulties involved and the clarity of the information provided. If necessary, the Council will seek further information from you.

8.8 Where any meeting is arranged, off-site if you so wish, you can be accompanied by a trade union or professional association representative or a friend.

8.9 The Council will take steps to minimise any difficulties which you may experience as a result of raising a concern. For instance, if you are required to give evidence in criminal or disciplinary proceedings the Council will arrange for you to receive advice about the procedure.

8.10 The Council accepts that you need to be assured that the matter has been properly addressed. Thus, subject to legal constraints, we will inform you of the outcome of any investigation.

9. THE RESPONSIBLE OFFICER

9.1 The Chief Executive has overall responsibility for the maintenance and operation of this Policy. That officer maintains a record of concerns raised and the outcomes (but

in a form which does not endanger your confidentiality) and will immediately notify the Monitoring Officer and Section 151 Officer of all issues raised under this Policy and will report as necessary to the Council.

10. HOW THE MATTER CAN BE TAKEN FURTHER

10.1 This Policy is intended to provide you with an avenue within the Council to raise concerns. The Council hopes you will be satisfied with any action taken. If you are not, and if you feel it is right to take the matter outside the Council, the following are possible contact points:

- one of the “prescribed persons”
- your trade union
- your local Citizens Advice Bureau
- relevant professional bodies or regulatory organisations
- a relevant voluntary organisation (Public Concern at Work - 020 7404 6609)
- the Police.

10.2 If you take the matter outside the Council, you should ensure that you do not disclose confidential information. Check with one of the Council’s nominated contact points about that (see 7.1).

11. Review

11.1 This policy will be reviewed annually and whenever the relevant legislation changes.

This page is intentionally left blank

RISK MANAGEMENT POLICY

Version No.	Author	Date	Summary of Changes
1		December 2014	
2		May 2016	
3	Andy Barton	May 2020	
4	Andy Barton	May 2021	
5	Andy Barton	May 2022	
6	Glenn Hammons	July 2023	Minor update to the importance of the role of internal audit in the Council's governance and assurance processes.

Version 6

July 2023

	Contents	Page No.
1.	Introduction	3
2.	Risk Management Structure	3
3.	Aims of the Policy	3
4.	Risk Management Policy	4
5.	Risk Appetite	6
6.	Corporate Risk Scrutiny Group	7
7.	Procedures	8
8.	Funding for Risk Management	8
9.	Benefits of Effective Risk Management	8
10.	Current Challenges Facing The Council	9
11.	Appendix A – Risk Management Framework	10

RISK MANAGEMENT POLICY

1. INTRODUCTION

1.1 The Council has adopted the principles of risk management in order to meet the following objectives:

- to protect the health, safety and welfare of its employees and the communities it serves;
- to protect its property, assets and other resources;
- to protect the services it provides; to main its reputation and good standing in the wider community; and
- to deliver its overall objectives and priorities.

2. RISK MANAGEMENT STRUCTURE

2.1 Risk Management is co-ordinated corporately by the Health and Safety Officer and through the Corporate Risk Scrutiny Group (RSG) chaired by Director of Resouces. It also refers and reports to Corporate Leadership Team thereby reaching all services in the Council and ensuring senior management oversight and involvement. Progress on Corporate Risk Management will be reported to members through performance reports to the Audit and Governance Committee. The Corporate Portfolio Holder is the Cabinet member with overall responsibility for risk management.

2.2 Risk management is embedded in the culture of the authority through:

- the continued adoption of the Council's risk management policy statement;
- a nominated officer lead, currently Director of Resources.
- the Corporate Risk Scrutiny Group and Corporate Leadership Team accountability;
- an established uniform procedure for the identification, analysis, management and monitoring of risk;
- training and briefings in conjunction with appropriate third parties and
- regular monitoring and reporting through the corporate performance management system and control mechanisms.

2.3 The Council is responsible for establishing and maintaining appropriate risk management processes, control systems, accounting records and governance arrangements. Internal Audit play a vital role in advising the Council that these arrangements are in place and operating effectively. Each year the Audit Manager produces a risk-based annual Audit Plan. This is informed by a risk assessment which includes a review of corporate and service risk registers, and consultation with key stakeholders and senior management. The Plan is developed to deliver a programme of internal audits to provide independent assurance to senior management and members. Internal audit undertake a risk based approach for individual assignments and gives a rating of the level of assurance that be awarded within each system / business area. This demonstrates the extent to which controls are operating effectively to ensure that significant risks to the achievement of the Council's priorities are being addressed.

3. AIMS OF THE POLICY

3.1 The Council will strive to maintain its diverse range of services to the community and visitors to the North West Leicestershire area. It will protect and continue to provide

these services by ensuring that its assets, both tangible and intangible, are protected against loss and damage. The Council is committed to a programme of risk management to ensure its ambitions for the community can be fulfilled through:

“The identification, analysis, management and financial control of those risks which can most impact on the Council’s ability to pursue its approved delivery plan”.

3.2 The Council is committed to using risk management to maintain and improve the quality of its own services as well as any contribution by partnerships through its community leadership role. The Risk Management Policy has the following aims and objectives:

- to continue to embed risk management into the culture of the Council;
- to promote the recognition of risk within the Council’s defined corporate aims and objectives;
- continue to raise risk awareness within the Council and its partners;
- to manage risk in accordance with best practice;
- to comply with legislation and guidance;
- to improving safety and increase safety awareness;
- to protect Council property, services and public reputation;
- to reduce disruption to services by having effective contingency or recovery plans in place to deal with incidents when they occur;
- to minimise injury, damage, loss and inconvenience to residents, staff, service users, assets, etc arising from or connected with the delivery of Council services;
- to review robust frameworks and procedures for the identification, analysis, assessment and management of risk, and the reporting and recording of events, based on best practice;
- to maximise value for money.

3.3 Regularly through the Corporate Risk Scrutiny Group, the Council’s Corporate Leadership Team (CLT) will review the Risk Management Policy and its risk management processes to ensure their continued relevance to the Council. The annual review will also assess performance against the aims and objectives set out above. Completion of the self- evaluation matrix will be a key monitoring tool and a central part of this review. CLT will be accountable to members for the effective management of risk within the Council. This will be achieved through the quarterly reporting of corporate risks to Audit and Governance Committee and at least annually to Cabinet.

4. RISK MANAGEMENT POLICY

4.1 The overall objective of the Council’s Risk Management Policy is to ensure that risks to the Council’s objectives, services, employees, partnerships and contractors are identified, recorded, amended, prioritised and then addressed by being treated, tolerated, transferred or terminated. The Policy incorporates:

(a) Identification / Consideration of Risks

- Identifies corporate and operational risks, assesses the risks for likelihood and impact, identifies mitigating controls and allocates responsibility for the mitigating controls.
- Requires the consideration of risk within all service plans and reviews and the regular review of existing risks as identified in the risk register.
- Requires, reports supporting strategic policy decisions and project initiation documents, to include a risk assessment.

- Externally horizon scan for impending risks that may impact the council, communicate the risk to the appropriate risk owner so they can assess for likelihood and impact, identify mitigating controls and allocate responsibility for themitigating controls.

(b) Development Delivery

- Allocates responsibility for embedding risk management to a senior officer and Member, to jointly champion.
- Embeds risk management into; strategic planning, financial planning, policy making and review, and performance management.
- Requires that an update report arising from the work of the Risk Scrutiny Group is presented to Corporate Leadership Team for discussion and information on a quarterly basis.
- Develops arrangements to monitor and measure performance of risk management activities against the Council's strategic aims and priorities.
- Considers risks in relation to significant partnerships, which requires assurances to be obtained about the management of those risks.

(c) Member Involvement / Responsibility

- Quarterly reports will be produced for Audit and Governance Committee on the management of business risks together with recommendation of appropriate actions.
- Reporting to Cabinet and Portfolio members where necessary.

(d) Training / Awareness

- Requires relevant training and tool kits to be given to appropriate staff to enable them to take responsibility for managing risks within their environment.
- Requires the maintenance of documented procedures for the control of risk and the provision of suitable information, training and supervision.
- Develops appropriate procedures and guidelines.
- Considers positive risks (opportunities) and negative risks (threats).
- Facilitates risk management awareness training for all members.

(e) Review

- Maintains and reviews a register of corporate business risks linking them to strategic business objectives and assigning ownership for each risk.
- Requires an annual review of the risk management process, including a report to CLT, localised Risk Registers where necessary and quarterly reporting to the Audit and Governance Committee.
- In the case of new or changing strategic risks, report to Audit and Governance Committee and/or Cabinet through the quarterly performance reporting process.
- Requires each team / department to review their individual Risk Registers as and when required (but no less than quarterly) managed by the respective CLT member.

(f) Business Continuity

- Develops contingency plans in areas where there is a potential for an occurrence having a catastrophic effect on the delivery of the Council's services.

(g) Insurance

- Ensures the appropriate officer responsible for insurance is notified of any new risks.
- Ensures adequate records are maintained and retained to support the Council's defence against disputed insurance claims.

(h) Controlling the Risks

Traditionally in risk management there are four ways to mitigate the risks to the organisation, these being typically referred to as **Treat, Tolerate, Transfer and Terminate** and are known collectively as the "4 Ts".

- **Tolerate** means the risk is known and accepted by the organisation. In such instances the senior management team should formally sign off that this course of action has been taken.
- **Transfer** means the risk mitigation is transferred i.e. it is passed to a third party such as an insurer or an outsourced provider, although it should be noted that responsibility for the risk cannot be transferred or eliminated.
- **Terminate** means we stop the process, activity, etc or stop using the premises, IT system, etc which is at risk and hence the risk is no longer relevant.
- **Treat** means we aim to reduce the likelihood of the threat materialising or else reduce the resultant impact through introducing relevant controls and continuity strategies.

5. RISK APPETITE

- 5.1 Our risk appetite guides how much risk we are willing to seek or accept to achieve our objectives. We recognise we will need to take risks, both in our ordinary business and to achieve the priorities set out in our Council Delivery Plan. Good risk management ensures we make well informed decisions, and we understand the associated risks. By ensuring that we properly respond to risks we will be more likely to achieve our priorities. It also provides control and a high level of due diligence consistent with our responsibilities in managing public money.
- 5.2 We recognise effective risk management considers not just threats but also opportunities. So, our approach to risk is to seek the right opportunities and, where possible, minimise threats. By encouraging managed risk taking and considering all of the available options we seek a balance between caution and innovation.
- 5.3 Our risk appetite reflects our current position; encouraging managed risk taking for minor to moderate level risks but controlling more closely those risks that come further up the scale. Our appetite for risk will vary over time depending on our ambitions and priorities and the environment we work in. Resources are aligned to priorities and arrangements are in place to monitor and mitigate risks to acceptable levels.
- 5.4 Beyond our risk appetite is our risk tolerance. This sets the level of risk that is unacceptable, whatever opportunities might follow. In such instances we will aim to reduce the risk to a level that is within our appetite. Whilst appetite may be lower, tolerance levels may be higher, and the Council recognises that it is not possible or necessarily desirable to eliminate some of the risks inherent in its activities. In some instances, acceptance of risk within the public sector is necessary due to the nature of services, constraints within operating environment and a limited ability to directly influence where risks are shared across sectors.

- 5.5 We illustrate our risk appetite and tolerance in our grading of risks within the risk register. Risks that are red represents the outer limit of our risk appetite, and those amber or green indicates the tolerance. Where risks are identified as red we will seek to reduce these risks through the 4 T's identified above. As a Council we are unlikely to take risks that will cause a significant negative consequence for our objectives, and only would consider doing so where this is a clear and overarching need to do so.

6. CORPORATE RISK SCRUTINY GROUP

- 6.1 The Corporate Risk Scrutiny Group is made up of technical experts and corporate leads from the Council's Service Areas. Members of the Group act as "champions" for risk within their services and the Group provides a link into the CLT.
- 6.2 The role of the Group is to maintain a formal framework that will assist with the management of risk and business continuity, by developing the corporate lead and advising CLT on the expected outcome. The objectives of the Group are:
- to assess and advise on the reduction of prevailing risks within the Council's services, to the benefit of staff and the public;
 - to discuss, agree and recommend as appropriate, on matters relating to corporate risk policy;
 - to make reports and recommendations to CLT;
 - to discuss operational risks insofar as they relate to matters of cross-directorate interest;
 - to oversee the implementation of the Council's Risk Management Policy, and to promote a holistic approach to its ongoing management;
 - to promote good risk management practices with the aim of reducing potential liabilities;
 - to consider and identify new risks, and ideas / schemes for risk reduction;
 - to provide a forum to discussion on risk management issues.

These will be achieved through the following:

- the use of the Council's Risk Management reporting system;
- monitoring the Risk Management Policy;
- reviewing the Council's risk register and associated action plans, acting as a forum for examining and rating risks and making recommendations to CLT;
- developing a comprehensive performance framework for risk management, and developing and using key indicators capable of showing improvements in risk management and providing early warning of risk;
- supporting the development and review of internal standards and procedures regarding significant risk areas;
- supporting the development and implementation of relevant training, awareness and education programmes;
- supporting the development and implementation of adequate, relevant and effective reporting, communication and information dissemination systems with managers and staff;
- supporting the effective monitoring and review of near misses, untoward incidents and accidents, legal and insurance claims and verifying that appropriate management action has been taken promptly to minimise the risk of future occurrence;
- supporting the review of the risk register and action plans to ensure that appropriate management action is taken appropriately to tolerate, treat, transfer or

- terminate the risk;
- monitoring compliance with legal and statutory duties;
- providing progress reports to CLT and members, drawing to their attention significant business risks;
- encouraging localised Risk Registers to be created where necessary, as well as supporting dynamic risk assessment.

7. PROCEDURES

- 7.1 The Council will adopt uniform procedures for the identification, analysis, management and monitoring of risk. These will be embodied in a formal risk management framework, which will be subject to annual review by the Audit and Governance Committee, following consideration by CLT.

The approved framework is set out in Appendix A to this Policy document.

8. FUNDING FOR RISK MANAGEMENT

- 8.1 The annual Service and Financial Planning process will include a review of operational risks and consider the allocation of funds for risk management initiatives as part of the annual budget process. If additional funds are required approval will be sought initially from CLT.

9. BENEFITS OF EFFECTIVE RISK MANAGEMENT

- 9.1 Effective risk management will deliver a number of tangible and intangible benefits to Individual services and to the Council as a whole e.g.

Improved Strategic Management

- Greater ability to deliver against objectives and targets
- Increased likelihood of change initiatives being delivered effectively
- Improved reputation, hence support for regeneration
- Increased confidence to take controlled risks

Improved Operational Managements

- Reduction in interruptions to service delivery: fewer surprises!
- Reduction in managerial time spent dealing with the consequences of a risk event occurring
- Improved health and safety of employees and others affected by the Council's activities
- Compliance with legislation and regulations

Improved Financial Management

- Better informed financial decision-making
- Enhanced financial control
- Reduction in the financial costs associated with losses due to service interruption, litigations, etc.
- Improved containment of insurance premiums

Improved Customer Service

- Minimal service disruption to customers and a positive external image

10. CURRENT CHALLENGES FACING THE COUNCIL

10.1 The Council provides a range of services to the residents of North West Leicestershire and the environment within which it operates is always evolving and changing. The current key challenges facing the Council include:

- Providing services through the cost of living crisis. This impacts on the Council from a cost pressure perspective as its cost base is increasing and from a service delivery perspective as there is greater demand for the services provided by the Council.
- Ensuring financial sustainability over the medium term.
- Embedding the new Council following the District elections in May 2023.
- Ensuring our business continuity and information technology security arrangements futureproof.
- Working with partners to establishing the East Midlands Freeport
- Keeping abreast of Government policy changes, for example the requirements of the recently created Office for Local Government.
- Continually developing our compliance and assurance frameworks to ensure robust decision making.

APPENDIX A

RISK MANAGEMENT FRAMEWORK

(A) What is the framework?

This framework promotes a set of uniform risk management procedures through which directorates will identify, analyse, monitor and manage the risks faced by the Council.

For the purposes of the framework, risk management is defined as *“the identification, analysis, management and financial control of those risks that can impact on the Council’s ability to deliver its services and priorities.”*

Risk management is therefore concerned with better decision making, through a clear understanding of all associated risks before final decisions are made by either members or officers. When risks are properly identified, analysed and prioritised it is possible to formulate action plans that propose management actions to reduce risk or deal adequately with the consequences of the risks should they occur. The underlying aim is to treat, terminate or transfer risk to bring them to an acceptable manageable level within the Council, monitor tolerated risk, ensuring services to the public can be maintained, and that the Council’s priorities can be fulfilled.

Risk management therefore supports the Council’s service planning process by positively identifying the key issues that could affect the delivery of the service objectives.

(B) Why does the Council need to consider risk management as part of its service planning?

All organisations have to deal with risks, whatever their nature. As a general principle the Council will seek to reduce or control all risks that have the potential to:

- harm individuals;
- affect the quality of service delivery or delivery of the council’s priorities;
- have a high potential of occurrence;
- would affect public confidence;
- would have an adverse effect on the council’s public image;
- would have significant financial consequences;
- have a potential for litigation in line with exposure detailed below.

Risk Management cannot therefore be considered in isolation, but needs to be an integral part of decision-making and service planning processes of the Council. Risk management must be fully embedded in:

- service planning,
- performance management,
- best value,
- committee reports.

For this reason risk management is located within the HR and Organisation Development team of the Council, with high level commitment by the Chief Executive to integrate risk management in everything the Council does.

(C) Assessing risk

Once risks have been identified, an assessment of their significance is required. This requires a robust and transparent scoring mechanism to be used uniformly across Council directorates.

Scoring should be a group exercise including managers and frontline employees. This is because people's perceptions vary and this can have an effect on scoring the risk. Employees who experience a risk every day can become complacent and fail to see how serious it may actually be, whilst a group will usually see the wider impact.

A decision on risk ownership is also required. The owner should be at management level and be responsible for ensuring that controls identified to manage the risk are in place and that they are effective. Delegation of responsibility for particular actions to other employees is acceptable, but overall control of risk must remain with management.

Tables 1 and 2 below set out a scoring mechanism for assessing the likelihood and the impact of exposure to risk.

Table 1 - assessing the likelihood of exposure

1. Low	Likely to occur once in every ten years or more
2. Medium	Likely to occur once in every two to three years
3. High	Likely to occur once a year
4. Very High	Likely to occur at least twice in a year

Table 2 - assessing the impact of exposure

1. Minor	Loss of a service for up to one day. Objectives of individuals are not met. No injuries. Financial loss over £1,000 and up to £10,000. No media attention. No breaches in Council working practices. No complaints / litigation.
2. Medium	Loss of a service for up to one week with limited impact on the general public. Service objectives of a service unit are not met. Injury to an employee or member of the public requiring medical treatment. Financial loss over £10,000 and up to £100,000. Adverse regional or local media attention - televised or news paper report. Potential for a complaint litigation possible. Breaches of regulations / standards.

3. Serious	<p>Loss of a critical service for one week or more with significant impact on the general public and partner organisations.</p> <p>Service objectives of the directorate of a critical nature are not met.</p> <p>Non-statutory duties are not achieved.</p> <p>Permanent injury to an employee or member of the public</p> <p>Financial loss over £100,000.</p> <p>Adverse national or regional media attention - national newspaper report.</p> <p>Litigation to be expected.</p> <p>Breaches of law punishable by fine.</p>
4. Major	<p>An incident so severe in its effects that a service or project will be unavailable permanently with a major impact on the general public and partner organisations.</p> <p>Strategic priorities of a critical nature are not met.</p> <p>Statutory duties are not achieved.</p> <p>Death of an employee or member of the public.</p> <p>Financial loss over £1m.</p> <p>Adverse national media attention - national televised news report.</p> <p>Litigation almost certain and difficult to defend.</p> <p>Breaches of law punishable by imprisonment.</p>

(D) Prioritisation of risk

Table 3 brings together in a matrix the likelihood and impact of risk.

Table 3 - a risk matrix

		Likelihood			
		1	2	3	4
Impact	4	4	8	12	16
	3	3	6	9	12
	2	2	4	6	8
	1	1	2	3	4

Based on this matrix, the Council must decide on the level of risk it is prepared to accept as part of its ongoing operations. Any risk above the agreed level should be considered unacceptable and will therefore need to be managed. The risks in the above matrix fall into three zones; red, amber and green. Table 4 sets out the Councils intended response to these risks.

Table 4 - intended responses to risk

Red	Controls and/or mitigating actions are required to reduce the risk to an acceptable level. Effort should be focused on reducing the risk of any items appearing in this zone, hence moving them to the amber or green zone.
Amber	Risks will require ongoing monitoring to ensure they do not move into the red zone. Depending on the resources required to address the red risks, it may be appropriate to develop controls/mitigating actions to control these risks.
Green	Existing controls and/or mitigating actions are sufficient and may be excessive. More resource committed to reduce these risks is likely to be wasted. Consideration should be given to relaxing the level of control to release resources for mitigating higher level risks.

(E) Format of the risk register

Annex 1 to this framework provides a standard format.

Corporate Risk Register													
Ref No.	Risk Description	Consequence	Cause	Inherent Risk			Responsibility of	Responsible to	Control Measures	Residual Risk			Movement of Risk
				Impact	Likelihood	Rating				Impact	Likelihood	Rating	

(F) Roles of Officers

The Council's work is delivered largely through its officers. Set out below is a summary of the roles of different groups of officers in the risk management process:

Lead officer – to oversee the overall risk management process and ensuring reporting to Audit & Governance Committee, Cabinet and if necessary, Council. Keep this Risk Management Policy under annual review.

CLT Members – to instil the importance of Risk Management as set out in this policy, to ensure that risk registers etc as set out in this policy are addressed in their areas of responsibility, and to take part in the overall management of risk across the authority.

Head of Human Resources & Organisational delivery – to address training needs related to the management of risk as they arise through Team Management plans and the coverage of risk training plan for the organisation as a whole.

Project sponsors – to ensure the projects under their sponsorship comply with the Risk Management Policy

Team Managers – to ensure risk management is instilled into Team Plans as they are developed and ensure that risk management is taken forward as part of the operation of their respective areas of control.

Members of Corporate Risk Scrutiny Group – to act as champions of risk in their service areas, and deliver the objectives of the group as set out in this policy.

All staff – to ensure that they are aware of risk management, the corporate policy regarding risk, and identify, report or manage risk as appropriate within their control.

This page is intentionally left blank

CORPORATE POLICY AND PROCEDURE ON THE REGULATION OF INVESTIGATORY POWERS ACT 2000 AND THE INVESTIGATOR POWERS ACT 2016

Version No.	Author	Date	Summary of Changes
See Page 19			
1.1	Kerryn Woolett	May 2020	
1.2	Kerryn Woolett	June 2021	
1.3	Kerryn Woollett	June 2022	No changes
1.4	Kerryn Woollett	June 2023	Change job title “Head of Legal and Commercial Services” to “Head of Legal and Support Services” Change Authorising Officers (para 8.6) to include Heads of Service to reflect change in constitution.

Version 1.4
June 2023

	Contents	Page No.
1.	Introduction	3
2.	Types of Surveillance	4
3.	Conduct and Use of Covert Human Intelligence Sources	5
4.	Open Source (Online) Covert Activity	6
5.	Use of Personal Devices for Business Use	7
6.	The Council Owned Drone	7
7.	Local Authority Directed Surveillance Crime Threshold	7
8.	Authorisation Process - Directed Surveillance and Use of a CHIS	7
9.	Communications Data	11
10.	Authorisation Process - Communications Data	12
11.	Central Co-ordination	16
12.	Working with Other Agencies	17
13.	Other Sources of Information	17
14.	Records Management	17
15.	Revision History	19

CORPORATE POLICY AND PROCEDURE ON THE REGULATION OF INVESTIGATORY POWERS ACT 2000 AND THE INVESTIGATORY POWERS ACT 2016

1. INTRODUCTION

- 1.1 The Regulation of Investigatory Powers Act 2000 (RIPA) is concerned with the regulation of surveillance and other intelligence gathering by public authorities in the conduct of their legitimate business.
- 1.2 The Investigatory Powers Act 2016 (IPA) sets out the extent to which certain investigatory powers may be used to interfere with privacy. In particular about the interception of communications, equipment interference and the acquisition and retention of **communications data**.
- 1.3 Section 6 of the Human Rights Act 1998 provides that it is unlawful for a public authority to act in a way which is incompatible with a European Convention right. Article 8 of the European Convention on Human Rights says that everyone has the right to respect for their private and family life, their home and their correspondence.
- 1.4 The use of surveillance and other intelligence gathering techniques may amount to an interference with rights protected by Article 8 of the European Convention on Human Rights and could amount to a violation of those rights unless the interference is in accordance with the law.
- 1.5 The aim of RIPA and the IPA is to provide a balance between preserving people's right to privacy and enabling enforcement agencies to gather evidence for effective enforcement action. RIPA provides a statutory framework for the authorisation of certain types of **covert** intelligence gathering which is consistent with the Human Rights Act 1998 and the European Convention on Human Rights. Similarly, the IPA provides a statutory framework for the lawful interception and use of **communications data**.
- 1.6 The Council has approved a policy for tackling fraud and corruption. In limited circumstances the Council may wish to use surveillance techniques or **communications data** for the purpose of enforcing this policy or other of its statutory functions. The requirements of RIPA and the IPA are most likely to apply to those sections of the Council with enforcement / investigatory functions.
- 1.7 Section 27 of RIPA provides that conduct authorised under RIPA will be "lawful for all purposes." This means a person authorised under RIPA is entitled to engage in the conduct which has been authorised under RIPA and the Council will be protected from challenges to both the gathering of, and the subsequent use of, covertly obtained information enabling the Council to show that it has acted lawfully.
- 1.8 RIPA also provides a statutory mechanism for authorising the use of a "**covert human intelligence source**", e.g. undercover agents.
- 1.9 The IPA permits access to **communications data** in specific circumstances.
- 1.10 Non-compliance with RIPA or the IPA may result in:
 - 1.10.1 evidence being disallowed by the courts;
 - 1.10.2 a complaint to the Investigatory Powers Commissioner's Office;

- 1.10.3 a complaint to the Local Government and Social Care Ombudsman; and/or
- 1.10.4 the Council being ordered to pay compensation.

It is essential therefore that the Council's policies and procedures, as set out in this document, are followed. A flowchart of the procedures to be followed is at Appendix 1.

2. TYPES OF SURVEILLANCE

- 2.1 Surveillance includes monitoring, observing, listening to persons, watching or following their movements, listening to their conversations and other such activities or communications. It also includes recording any of the aforementioned activities.
- 2.2 Surveillance may be "**overt**" or "**covert**".
- 2.3 Surveillance will be "**overt**" if the act of surveillance is not calculated to be hidden from view, even if the motives of the person undertaking the surveillance remain concealed.
- 2.4 Most of the surveillance carried out by the Council is done overtly – there is nothing secretive, clandestine or hidden about it. In many cases, officers will be behaving in the same way as a normal member of the public, and/or will be going about Council business openly. Similarly, surveillance will be **overt** if the subject has been told it will happen (e.g. where a noisy householder is warned that noise will be recorded if it continues).
- 2.5 Surveillance is "**covert**" if, and only if, it is carried out in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is or may be taking place. RIPA regulates two types of **covert** surveillance.
- 2.6 The first type of **covert** surveillance is "**directed surveillance**". "**Directed surveillance**" means surveillance that is:
 - 2.6.1 **covert**;
 - 2.6.2 not intrusive;
 - 2.6.3 undertaken for the purposes of a specific investigation or specific operation;
 - 2.6.4 undertaken in such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation); and
 - 2.6.5 undertaken otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under RIPA to be sought for the carrying out of the surveillance.
- 2.7 RIPA states that "**private information**" includes any information relating to a person's private or family life. The Home Office Covert Surveillance and Property Interference Revised Code of Practice (latest edition at time of writing was August 2018) states that as a result, "**private information**" is capable of including any aspect of a person's private or personal relationship with others, such as family (which should be treated as extending beyond the formal relationships created by marriage or civil partnership) and professional or business relationships.

- 2.8 RIPA sets out a number of grounds on which an authorisation for **directed surveillance** can be considered necessary. In the case of a Local Authority, only one of these grounds is applicable, that ground is that **directed surveillance** is necessary “for the purpose of preventing or detecting crime or of preventing disorder”.
- 2.9 The fact that **covert** surveillance occurs in a public place or on business premises does not mean that it cannot result in the obtaining of private information about a person. Prolonged surveillance targeted on a single person will usually result in the obtaining of private information about that person as well as others that he or she comes into contact or associates with.
- 2.10 An example of **directed surveillance** would be when officers follow a person over a period of time to find out whether they are working at the same time as claiming benefit. Similarly, although town centre CCTV cameras will not normally require a RIPA authorisation, if a camera is directed in such a way as to observe a particular individual, this would amount to **directed surveillance** and an authorisation would be required.
- 2.11 The second type of **covert** surveillance is “**intrusive surveillance**”. Surveillance is intrusive if, and only if, it is **covert** surveillance that is carried out in relation to anything taking place on any residential premises or in any private vehicle and involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.
- 2.12 A Local Authority cannot carry out **intrusive surveillance** under RIPA. **Intrusive surveillance** can only be carried out by the police and other law enforcement agencies.

3. CONDUCT AND USE OF COVERT HUMAN INTELLIGENCE SOURCES

- 3.1 A person is a **Covert Human Intelligence Source (CHIS)** if he or she establishes or maintains a personal or other relationship with another person in order to covertly obtain or disclose information.
- 3.2 RIPA sets out special rules relating to the management and use of information supplied by a **CHIS** and a duty of care is owed to the **CHIS** in how the information is used.
- 3.3 The conduct or use of a **CHIS** requires prior authorisation. Again, the ground on which a **CHIS** may be used by a Local Authority is “for the purpose of preventing or detecting crime or of preventing disorder.”
- 3.4 A RIPA authorisation may not be required in circumstances where members of the public volunteer information to the Council as part of their normal civic responsibilities, however, this will depend on how the information has been obtained. If the person has obtained the information as an ‘insider’ i.e. in the course of a personal or other relationship or “as a result of the existence of such a relationship” then the person is likely to be a **CHIS**, even if the relationship was not formed or maintained for that purpose.
- 3.5 If the person has obtained the information as an outside observer then he or she is not a **CHIS**.
- 3.6 Where contact numbers are set up by the Council to receive information then it is unlikely that persons reporting information will be **CHISs** and similarly, people who complain about anti- social behaviour, and are asked to keep a diary, will not normally

be **CHISs** because they are not being required to establish or maintain a relationship for a **covert** purpose.

Juvenile CHISs

- 3.7 Special safeguards apply to the use or conduct of juveniles, that is, those under 18 years old, as a **CHIS**. On no occasion should the use or conduct of a **CHIS** under 16 years of age be authorised to give information against their parents or any person who has parental responsibility for them. In other cases, authorisations should not be granted unless the special provisions, contained within the Regulation of Investigatory Powers (Juveniles) Order 2000 (as amended), are satisfied.
- 3.8 Authorisations for juvenile sources should be granted by those listed in the table at Annex A of the Home Office Covert Human Intelligence Sources Revised Code of Practice (latest edition at time of writing was August 2018). In this Council, only the Chief Executive may authorise the use of a juvenile or vulnerable individual as a CHIS. The duration of such an authorisation is four months from the time of grant or renewal (instead of twelve months), and the authorisation should be subject to at least monthly review. For the purpose of these rules, the age test is applied at the time of the grant or renewal of the authorisation.

4. OPEN SOURCE (ONLINE) COVERT ACTIVITY

- 4.1 The use of the internet may be required to gather information during an operation, which may amount to **directed surveillance**. The Home Office Covert Surveillance and Property Interference Revised Code of Practice (latest edition at time of writing was August 2018) advises that simple reconnaissance of websites, that is, preliminary examination with a view to establishing whether a site or its contents are of interest, is unlikely to interfere with a person's reasonably held expectation of privacy and therefore is not likely to require a **directed surveillance** authorisation. However, where there is an intention to use the internet as part of an investigation and private information is likely to be obtained, a RIPA authorisation should be considered. When conducting an investigation which involves the use of the internet factors to consider are:
- officers must not create a false identity in order to "befriend" individuals on social networks without an authorisation under RIPA;
 - officers viewing an individual's public profile on a social network should do so only to the minimum degree necessary and proportionate in order to obtain evidence to support or refute the suspicions or allegations under investigation;
 - repeated viewing of open profiles on social networks to gather evidence or to monitor an individual's status, must only take place once a RIPA authorisation has been granted and approved by a Magistrate; and
 - officers should be aware that it may not be possible to verify the accuracy of information on social networks and, if such information is to be used as evidence, take reasonable steps to ensure its validity.
- 4.2 Further, where an investigator may need to communicate covertly online, for example, contacting individuals using social media websites without disclosing his or her identity, a **CHIS** authorisation should be considered.

5. USE OF PERSONAL DEVICES FOR BUSINESS USE

- 5.1 Use of a personal device to access the internet or social media for business use, for example, as part of investigation, is still captured by RIPA. Consequently, officers are advised not to use personal devices for business use, particularly using a personal device to access the internet and social media for business use.

6. THE COUNCIL OWNED DRONE

- 6.1 Use of a drone has the potential to capture **private information**. **Collateral intrusion** is also highly likely when using a drone. Therefore, consideration should be given to whether a RIPA authorisation is required. A drone can be a very useful tool to use in an investigation, however, if there is the potential to gather **personal information** the subject of the investigation and/or the landowner will either need to be notified of the use of the drone (such that any use of the drone is not covert) or a RIPA authorisation will be needed. If the drone is to be flown over a residential area or highly populated area, where the potential for **collateral intrusion** is high, notification that the drone will be used will be published on the Council's website prior to the flight.

7. LOCAL AUTHORITY DIRECTED SURVEILLANCE CRIME THRESHOLD

- 7.1 A **Crime Threshold** applies to the authorisation of **directed surveillance** by Local Authorities under RIPA (see article 7A of the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010). This **Crime Threshold** does not apply to the authorisation of a **CHIS** by a Local Authority.
- 7.2 Local Authorities can only authorise use of **directed surveillance** under RIPA for the purpose of preventing or detecting criminal offences or disorder associated with criminal offences that are:
- 7.2.1 punishable, whether on summary conviction or on indictment, by a maximum term of at least six months imprisonment; or
- 7.2.2 relate to the underage sale of alcohol or tobacco.
- 7.3 If the **Crime Threshold** is not met, though surveillance is still required, a Non-RIPA form should be completed. A Non-RIPA form requires the applicant officer to consider necessity and proportionality as per a RIPA authorisation, however, there is no requirement for approval by a Justice of the Peace.

8. AUTHORISATION PROCESS - DIRECTED SURVEILLANCE AND USE OF A CHIS

Stage 1 - Request for Authorisation

- 8.1 **Directed surveillance** or the use of a **CHIS** can only be authorised by a Local Authority if the authorisation is *necessary* for the purpose of preventing or detecting crime or preventing disorder and the authorised surveillance is *proportionate* to what is sought to be achieved by carrying the surveillance out. When authorising the use of a **CHIS** arrangements also need to be in place for management of the **CHIS** and to ensure the security and welfare of the **CHIS**.
- 8.2 For **directed surveillance** or the use of a **CHIS**, only the approved RIPA forms, available on the Home Office website

(<https://www.gov.uk/government/collections/ripa-forms--2>)

may be used. Any other form will be rejected by the Authorising Officer. The applicant officer should complete the appropriate form providing as much detail as possible then submit to the appropriate Authorising Officer for authorisation.

- 8.3 If in doubt about the process to be followed or the information required in the form, an applicant officer should always seek the advice of the Head of Legal and Support Services or the Audit Manager before applying for an authorisation under RIPA.
- 8.4 The applicant officer will be responsible for ensuring that copies of all forms are forwarded to the Audit Manager within seven days of issue. As a control measure the Audit Manager will supply the applicant officer with a referenced copy of the authorisation which they should keep in their department in secure storage. Officers should ensure that material passing between them is sent in such a way that it cannot be read or intercepted by other people.

Stage 2 - Considering an Application for Authorisation

- 8.5 **Directed surveillance** or use of a **CHIS** can only be lawfully carried out if properly authorised and carried out in strict accordance with the terms of the authorisation.
- 8.6 The Secretary of State has specified by statutory instrument (the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010) that, for any district council in England, Directors, Heads of Service or Service Managers or equivalent are designated persons for the purpose of s.28 and s.29 of RIPA, that is, they may act as Authorising Officers for the purpose of authorising applications for **directed surveillance** or the use of a **CHIS**. In this Council, the Chief Executive, the Directors and Heads of Service are designated to act as Authorising Officers under the Constitution (Part 2, Sec G4, Para 1.5).
- 8.7 Before signing a form seeking authorisation, the Authorising Officer must have regard to this Policy and Procedure, to any relevant Code of Practice, to any advice from the Head of Legal and Support Services or the Audit Manager and to any other relevant guidance.
- 8.8 The Authorising Officer must also satisfy himself / herself that the surveillance proposed in the application is:
 - 8.8.1 *in accordance with the law;*
 - 8.8.2 *necessary* in the circumstances of the particular case on the ground of preventing or detecting crime or preventing disorder; and
 - 8.8.3 *proportionate* to what it seeks to achieve.
- 8.9 In considering whether or not the proposed surveillance is proportionate, the Authorising Officer will need to consider:
 - 8.9.1 The seriousness of the crime or disorder which the surveillance seeks to detect and weigh this against the type and extent of surveillance proposed. For minor offences, it may be that surveillance is never proportionate; and

- 8.9.2 whether there are other more non- intrusive ways of achieving the desired outcome. If there are none, the Authorising Officer will need to consider whether the proposed surveillance is no more than necessary to achieve the objective, as the least intrusive method will be considered proportionate by the courts.
- 8.10 The Authorising Officer will also need to take into account the risk of intrusion into the privacy of persons other than the specified subject of the surveillance. This is known as “**collateral intrusion**”. Measures must be taken whenever practicable to avoid or minimise, so far as practicable, **collateral intrusion**.
- 8.11 When authorising the conduct or use of a **CHIS** the Authorising Officer must also be satisfied that appropriate arrangements are in place for the management and oversight of the **CHIS**. This must address health and safety issues through a risk assessment. The Authorising Officer must also have regard to any adverse impact on community confidence that may result from the use or conduct of the information obtained.
- 8.12 The authorisation does not take effect until a Justice of the Peace has made an order approving the grant of the authorisation.

Stage 3 - Judicial Approval

- 8.13 If the Authorising Officer is satisfied that the surveillance is *necessary and proportionate*, they will instruct Legal Services to seek approval from a Justice of the Peace sitting at the Magistrates’ Court.
- 8.14 Legal Services will request a hearing date from the Court. The time taken to obtain a hearing date from the Court will need to be taken into account when scheduling any proposed surveillance.
- 8.15 Urgent approvals should not be necessary.
- 8.16 If the approval is urgent and cannot be handled the next working day then the applicant officer should:
- 8.16.1 phone the Court’s out of hours legal staff contact. You will be asked about the basic facts and urgency of the authorisation. If the police are involved in the investigation you will need to address why the police cannot authorise the application.
- 8.16.2 If urgency is agreed, then arrangements will be made for a suitable Magistrate to consider the application. You will be told where to attend and give evidence.
- 8.16.3 Attend the hearing as directed with two copies of the signed RIPA authorisation form.
- 8.17 At the hearing the Council will provide the Court with a copy of the authorisation signed by the Authorising Officer, together with any supporting documents relevant to the matter showing the necessity and proportionality of the authorisation and which contain all the information relied upon. Also included will be a summary of the circumstances of the case.
- 8.18 The hearing will be in private heard by a single Justice of the Peace (Magistrate / District Judge) who will read and consider the application.
- 8.19 On reviewing the papers and hearing the application the Justice of the Peace will determine whether they are satisfied that there were, at the time the authorisation was granted, and continue to be reasonable grounds for believing that the authorisation is

necessary and proportionate. In addition they must also be satisfied that the Authorising Officer had the relevant authority to authorise the Council's own internal authorisation prior to it passing to the Court.

- 8.20 For authorisations for the use of a **CHIS** the Justice of the Peace will also need to be satisfied that there were and are reasonable grounds for believing appropriate arrangements are in place for the management and oversight of the **CHIS**.
- 8.21 The Justice of the Peace may ask questions of the Council in order to satisfy themselves of the necessity and proportionality of the request.
- 8.22 In considering the application the Justice of the Peace may decide to:
 - 8.22.1 grant an Order approving the authorisation or renewal. The authorisation or renewal will then take effect and the Local Authority may proceed to use surveillance in accordance with the authorisation;
 - 8.22.2 refuse to approve the authorisation or renewal. The RIPA authorisation will not take effect and the Local Authority may not use the proposed surveillance. Where an application has been refused the Council may wish to consider the reasons for that refusal. For example, a technical error in the form may be remedied without the need to go through the internal authorisation process again. The Council may then wish to reapply for judicial approval once those errors have been remedied;
 - 8.22.3 refuse to approve the grant or renewal and quash the authorisation or notice. A Justice of the Peace must not exercise its power to quash an authorisation unless the applicant (the Council) has had at least two business days' notice from the date of the refusal in which to make representations.

Stage 4 - Duration and Review

- 8.23 If the Justice of the Peace approves the authorisation, the authorisation will last, in the case of **directed surveillance**, a period of 3 months and, in the case of a **CHIS**, a period of 12 months.
- 8.24 Authorising Officers must then conduct regular reviews of authorisations granted in order to assess the need for the surveillance to continue. Reviews should be conducted on a monthly basis as a minimum. The Authorising Officer may decide that reviews should be conducted more frequently, particularly where a high level of collateral intrusion is likely.
- 8.25 A review involves consultation with the applicant officer and any other persons involved in the surveillance. The applicant officer must give sufficient information about the surveillance and any information obtained by the surveillance for the Authorising Officer to be satisfied that the authorised surveillance should continue. Applicant officers should be pro-active in preparing reports to assist Authorising Officers carry out reviews.

Stage 5 - Renewals

- 8.26 If it appears that the surveillance will continue to be *necessary* and *proportionate* beyond the 3 month period for **directed surveillance** or 12 months for use of a **CHIS**, the authorisation must be renewed.
- 8.27 An application for renewal should be made by the applicant officer by completing the appropriate form which is available from the Home Office website (<https://www.gov.uk/government/collections/ripa-forms--2>). This form should then be submitted to the Authorising Officer who must then consider the matter afresh, including taking into account the benefits of the surveillance to date and any collateral intrusion that has occurred.
- 8.28 The Authorising Officer must be satisfied that it is *necessary* and *proportionate* for the authorisation to continue and that the **Crime Threshold** continues to be met. The authorisation for renewal must then be approved by a Justice of the Peace for it to take effect.
- 8.29 An authorisation may be renewed and approved before the initial authorisation ceases to have effect but the renewal takes effect from the time at which the authorisation would have expired. If necessary, a renewal can be granted more than once.

Stage 6 - Cancellations

- 8.30 The Authorising Officer who granted or last renewed the authorisation must cancel the authorisation if the grounds for granting (or renewing) no longer apply or if the authorisation is no longer *necessary* or *proportionate*.
- 8.31 An authorisation can be cancelled on the initiative of the Authorising Officer following a periodic review or after receiving an application for cancellation from the applicant officer. Forms for the cancellation of **directed surveillance** and use of a **CHIS** are available on the Home Office website

(<https://www.gov.uk/government/collections/ripa-forms--2>)

9. COMMUNICATIONS DATA

- 9.1 The term “**communications data**” includes the “who”, “when”, “where”, and “how” of a communication but not the content i.e. what was said or written. It includes the way in which, and by what method, a person or thing communicates with another person or thing. It excludes anything within a communication including text, audio and video that reveals the meaning, other than inferred meaning, of the communication.
- 9.2 It can include the address to which a letter is sent, the time and duration of a communication, the telephone number or e-mail address of the originator and recipient, and the location of the device from which the communication was made. It covers electronic communications including internet access, internet telephony, instant messaging and the use of applications. It also includes postal services.
- 9.3 The acquisition of **communications data** is permitted under Part 3 of the IPA and will be a justifiable interference with an individual’s human rights under the European Convention on Human Rights only if the conduct being authorised or required to take place is *necessary* for the purposes of a specific investigation or operation, *proportionate* and *in accordance with law*.
- 9.4 Training should be made available to all those who participate in the acquisition and disclosure of **communications data**.

- 9.5 The Home Office has published the “Communications Data Code of Practice” (latest edition at time of writing was November 2018). This code should be readily available to persons involved in the acquisition of **communications data** under the IPA and persons exercising any functions to which this code relates must have regard to the code.
- 9.6 The IPA stipulates that conduct to be authorised must be *necessary* for one or more of the purposes set out in the IPA. For Local Authorities this purpose is “for the applicable crime purpose” which means:
- 9.6.1 where the **communications data** is wholly or partly events data (events data covers information about time-bound events taking place across a telecommunication system at a time interval, for example, information tracing the origin or destination of a communication that is, or has been, in transmission), the purpose of preventing or detecting serious crime; or
- 9.6.2 in any other case, the purpose of preventing or detecting crime or of preventing disorder.
- 9.7 “Serious Crime” means:
- 9.7.1 an offence for which an adult is capable of being sentenced to one year or more in prison;
- 9.7.2 any offence involving violence, resulting in a substantial financial gain or involving conduct by a large group of persons in pursuit of a common goal;
- 9.7.3 any offence committed by a body corporate;
- 9.7.4 any offence which involves the sending of a communication or a breach of privacy; or
- 9.7.5 an offence which involves, as an integral part of it, or the sending of a communication or breach of a person’s privacy.
- 9.8 A Local Authority may not make an application that requires the processing or disclosure of internet connection records for any purpose.

10. AUTHORISATION PROCESS - COMMUNICATIONS DATA

- 10.1 Acquisition of **communications data** under the IPA involves four roles:
- 10.1.1 The Applicant Officer - The applicant officer is a person involved in conducting or assisting an investigation or operation within a relevant public authority who makes an application in writing or electronically for the acquisition of **communications data**;
- 10.1.2 The Single Point of Contact (SPoC) - The SPoC is an individual trained to facilitate the lawful acquisition of **communications data** and effective co-operation between a public authority, the Office for Communications Data Authorisations (OCDA) and telecommunications operators and postal operators. To become accredited an individual must complete a course of training appropriate for the role of a SPoC and have been issued the relevant SPoC unique identifier. The Home Office provides authentication services to enable telecommunications operators and postal operators to validate SPoC credentials;

- 10.1.3 The Senior Responsible Officer - Within every relevant public authority there should be a Senior Responsible Officer. The Senior Responsible Officer must be of a senior rank in a public authority. This must be at least the same rank as the designated senior officer specified in Schedule 4 of the IPA. Where no designated senior officer is specified the rank of the senior responsible officer must be agreed with the Home Office; and
- 10.1.4 The Authorising Individual - **Communications data** applications can be authorised by three separate categories of individual depending on the circumstances of the specific case. The Authorising Individual for Local Authorities is the authorising officer in the OCDA. Section 60A of the IPA confers power on the IPC to authorise certain applications for **communications data**. In practice the IPC will delegate these functions to his staff. These staff will sit in a body which is known as the OCDA.
- 10.2 An authorisation provides for persons within a public authority to engage in conduct relating to a postal service or telecommunication system, or to data derived from such a telecommunication system, to obtain **communications data**. The following types of conduct may be authorised:
- 10.2.1 conduct to acquire **communications data** - which may include the public authority obtaining **communications data** themselves or asking any person believed to be in possession of or capable of obtaining the **communications data** to obtain and disclose it; and/or
- 10.2.2 the giving of a notice - allowing the public authority to require by a notice a telecommunications operator to obtain and disclose the required data.

Stage 1 - Making an Application

- 10.3 Before public authorities can acquire **communications data**, authorisation must be given by an Authorising Individual. An application for that authorisation must include an explanation of the necessity of the application.
- 10.4 Necessity should be a short explanation of the investigation or operation, the person and the **communications data** and how these three link together. The application must establish the link between the three aspects to be able to demonstrate the acquisition of **communications data** is necessary for the statutory purpose specified.
- 10.5 When granting an authorisation the authorising individual must also believe that conduct to be proportionate to what is sought to be achieved by obtaining the specified **communications data** – that the conduct is no more than is required in the circumstances. This involves balancing the extent of the interference with an individual's rights and freedoms against a specific benefit to the investigation or operation being undertaken by a relevant public authority in the public interest.
- 10.6 As well as consideration of the rights of the individual whose data is to be acquired consideration must also be given to any actual or potential infringement of the privacy and other rights of individuals who are not the subject of the investigation or operation.
- 10.7 The applicant officer will complete an application form setting out for consideration the necessity and proportionality of a specific requirement for acquiring **communications data**.

- 10.8 The application should record subsequently whether it was authorised by an authorising individual and when that decision was made. Applications should be retained by the public authority and be accessible to the SPoC.

Stage - 2 Consultation with the Single Point of Contact

- 10.9 A SPoC must be consulted on all Local Authority applications before they are authorised.
- 10.10 Amongst other things the SPoC will:
- 10.10.1 assess whether the acquisition of specific **communications data** from a telecommunications operator or postal operator is reasonably practicable or whether the specific data required is inextricably linked to other data; and
- 10.10.2 advise applicants on the most appropriate methodology for acquisition of data where the data sought engages a number of telecommunications operators or postal operators.
- 10.11 The National Anti-Fraud Network ('NAFN') is hosted by Tameside Metropolitan Borough Council.
- 10.12 In accordance with section 73 of the IPA, all Local Authorities who wish to acquire **communications data** under the IPA must be party to a collaboration agreement. In practice this means they will be required to become members of NAFN and use NAFN's shared SPoC services. Applicant officers within Local Authorities are therefore required to consult a NAFN SPoC throughout the application process. The accredited SPoCs at NAFN will scrutinise the applications independently. They will provide advice to the Local Authority ensuring it acts in an informed and lawful manner.
- 10.13 In addition to being considered by a NAFN SPoC, the local authority making the application must ensure someone of at least the rank of the senior responsible officer in the local authority is aware the application is being made before it is submitted to an authorising officer in OCDA. The local authority senior responsible officer must be satisfied that the officer(s) verifying the application is (are) of an appropriate rank and must inform NAFN of such nominations. In this Council the Chief Executive is the Senior Responsible Officer and the officers notified to the NAFN (notified in March 2019) as able to verify applications are the Head of Legal and Support Services and the Audit Manager.
- 10.14 NAFN will be responsible for submitting the application to OCDA on behalf of the local authority.

Stage 3 - Authorisation of Applications

- 10.15 The (OCDA) performs this function on behalf of the IPC. An authorising officer in OCDA can authorise requests from Local Authorities.
- 10.16 The authorising individual is responsible for considering and, where appropriate, authorising an application for **communications data**. It is their responsibility to consider the application and record their considerations at the time, in writing or electronically in order to show that they have understood the need for the application and considered necessity and proportionality to a standard that will withstand scrutiny. Comments should be tailored to a specific application as this best demonstrates the application has been properly considered.

- 10.17 If the authorising individual believes the acquisition of **communications data** meets the requirements set out in the IPA and is necessary and proportionate in the specific circumstances, an authorisation will be granted. If the authorising individual does not consider the criteria for obtaining the data have been met the application should be rejected and/or referred back to the SPoC and the applicant officer.

Stage 4 - Refusal to Grant an Authorisation

- 10.18 Where a request is refused by an authorising officer in OCDA, the public authority has three options:
- 10.18.1 not proceed with the request;
- 10.18.2 resubmit the application with a revised justification and/or a revised course of conduct to acquire **communications data**; or
- 10.18.3 resubmit the application with the same justification and same course of conduct seeking a review of the decision by OCDA. A public authority may only resubmit an application on the same grounds to OCDA where the senior responsible officer or a person of equivalent grade in the public authority has agreed to this course of action. OCDA will provide guidance on its process for reviewing such decisions.

Stage 5 - Duration of Authorisations and Notices

- 10.19 An authorisation becomes valid on the date upon which the authorisation is granted. It is then valid for a maximum of one month. This means the conduct authorised should have been commenced, which may include the giving of a notice, within that month.
- 10.20 Any notice given under an authorisation remains in force until complied with or until the authorisation under which it was given is cancelled.
- 10.21 All authorisations should refer to the acquisition or disclosure of data relating to a specific date(s) or period(s). Any period should be clearly indicated in the authorisation. The start date and end date should be given, and where a precise start and end time are relevant these must be specified.
- 10.22 Where an authorisation relates to the acquisition or obtaining of specific data that will or may be generated in the future, the future period is restricted to no more than one month from the date upon which the authorisation was granted.
- 10.23 Authorising individuals should specify the shortest possible period of time for any authorisation. To do otherwise would impact on the proportionality of the authorisation and impose an unnecessary burden upon the relevant telecommunications operator(s) or postal operator(s).

Stage 6 - Renewal of Authorisations

- 10.24 Any valid authorisation may be renewed for a period of up to one month by the grant of a further authorisation. A renewed authorisation takes effect upon the expiry of the authorisation it is renewing.
- 10.25 Renewal may be appropriate where there is a continuing requirement to acquire or obtain data that will or may be generated in the future. The reasons for seeking renewal

should be set out by the applicant officer in an addendum to the application upon which the authorisation being renewed was granted.

10.26 Where an authorising individual is granting a further authorisation to renew an earlier authorisation, they should:

10.26.1 consider the reasons why it is necessary and proportionate to continue with the acquisition of the data being generated; and

10.26.2 record the date and, when appropriate to do so, the time when the authorisation is renewed.

Stage 7 - Cancellations

10.27 An authorisation may be cancelled at any time by the Local Authority or OCDA and must be cancelled if, at any time after the granting of the authorisation, it is no longer necessary for a statutory purpose or the conduct required by the authorisation is no longer proportionate to what was sought to be achieved.

10.28 In practice, it is likely to be the public authority that is first aware that the authorisation is no longer necessary or proportionate. In such cases the SPoC (having been contacted by the applicant officer, where appropriate) must cease the authorised conduct.

10.29 A notice given under an authorisation (and any requirement imposed by a notice) is cancelled if the authorisation is cancelled but is not affected by the authorisation ceasing to have effect at the end of one month period of validity.

11. CENTRAL CO-ORDINATION

11.1 The Chief Executive will be the Senior Responsible Officer for the overall implementation of RIPA and the IPA.

11.2 The Head of Legal and Support Services will be responsible for:

11.2.1 giving advice and assistance to all staff concerned with the operation of RIPA and the IPA;

11.2.2 arranging training for all staff concerned with the operation of RIPA and the IPA; and

11.2.3 maintaining and keeping up to date this corporate policy and procedure.

11.3 The Audit Manager will be responsible for:

11.3.1 maintaining a central and up to date record of all authorisations;

11.3.2 along with the Head of Legal and Support Services, giving advice and assistance to all staff concerned with the operation of RIPA and the IPA; and

11.3.3 allocating reference numbers to authorisations.

12. WORKING WITH OTHER AGENCIES

12.1 When another agency has been instructed on behalf of the Council to undertake any action under RIPA, this Council will be responsible for obtaining a RIPA authorisation and therefore this Policy and Procedure must be used. The other agency must then be given explicit instructions on what actions it may undertake and how these actions are to be undertaken.

12.2 When another agency (e.g. Police, HMRC, etc):

12.2.1 wish to use the Council's resources (e.g. CCTV surveillance systems) for RIPA purposes, that agency must use its own RIPA procedures and, before any officer agrees to allow the Council's resources to be used for the other agency's purposes he or she must obtain a copy of that agency's RIPA form, a copy of which must be passed to the Audit Manager for inclusion on the central register;

12.2.2 wish to use the Council's premises for their own RIPA action, and is expressly seeking assistance from the Council, the request should normally be granted unless there are security or other good operational or managerial reasons as to why the Council's premises should not be used for the other agency's activities. Suitable insurance or other appropriate indemnities may need to be sought. In such cases, the Council's own RIPA forms should not be used as the Council is only assisting and not involved in the RIPA activity of the other agency.

13. OTHER SOURCES OF INFORMATION

13.1 The Home Office has issued Codes of Practice on **directed surveillance, CHISs and communications data**. These Codes of Practice supplement this policy and procedure document and should be used as a source of reference by all officers whose task it is to apply the provisions of RIPA and the IPA and their subordinate legislation.

14. RECORDS MANAGEMENT

14.1 The Council must keep a detailed record of all authorisations, judicial approvals, reviews, renewals, cancellations and rejections in the relevant services. A central record of all authorisation forms, whether authorised or rejected, will be maintained and monitored by the Audit Manager.

14.2 All Authorising Officers must send all original applications for authorisation to the Audit Manager. Each document will be given a unique reference number, the original will be placed on the central record and a copy will be returned to the applicant officer.

14.3 Copies of all other forms used and the judicial approval form must be sent to the Audit Manager bearing the reference number previously given to the application to which it refers.

Service Records

14.4 Each service must keep a written record of all authorisations issued to it, and any judicial approvals granted, to include the following:

14.4.1 a copy of the application and a copy of the authorisation together with any supplementary documentation and notification of the approval given by the Authorising Officer;

14.4.2 a record of the period over which the operation has taken place;

- 14.4.3 the frequency of reviews prescribed by the Authorising Officer;
- 14.4.4 a record of the result of each review;
- 14.4.5 a copy of any renewal of an authorisation and any supporting documentation submitted when the renewal was requested;
- 14.4.6 the date and time when any instruction was given by the Authorising Officer, including cancellation of such authorisation;
- 14.4.7 a copy of the order approving or otherwise the grant or renewal of an authorisation from a Justice of the Peace; and
- 14.4.8 the required date of destruction and when this was completed.

Central Record Maintained by the Audit Manager

- 14.5 A central record of all authorisation forms, whether authorised or rejected, is kept by the Audit Manager. The central record must be readily available for inspection on request by the Investigatory Powers Commissioner.
- 14.6 The central record must be updated whenever an authorisation is granted, reviewed, renewed or cancelled. Records will be reviewed after a period of 6 years from the date on which the relevant criminal or civil proceedings file is closed for archive and deleted when no longer necessary.
- 14.7 The central record must contain the following information:
 - 14.7.1 the type of authorisation;
 - 14.7.2 the date on which the authorisation was given;
 - 14.7.3 name / rank of the Authorising Officer;
 - 14.7.4 details of attendances at the Magistrates' Court to include date of attendances at court, the determining Justice of the Peace, the decision of the Justice of the Peace and the time and date of that decision;
 - 14.7.5 the unique reference number (URN) of the investigation / operation. This will be issued by the Audit Manager when a new application is entered in the Central Record. The applicant officer will be informed accordingly and should use the same URN when requesting a renewal or cancellation;
 - 14.7.6 the title of the investigation / operation, including a brief description and names of the subjects, if known;
 - 14.7.7 if the authorisation was renewed, when it was renewed and who authorised the renewal, including the name and rank / grade of the Authorising Officer;
 - 14.7.8 whether the investigation / operation is likely to result in the obtaining of **confidential information** (information is confidential if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation. Examples might include consultations between a health professional and a patient, information from a patient's medical records; or matters subject to legal privilege);

- 14.7.9 if the authorisation was reviewed, when it was reviewed and who authorised the review, including the name and rank / grade of the Authorising Officer;
- 14.7.10 the date and time that the authorisation was cancelled.
- 14.8 It should also contain a comments section enabling oversight remarks to be included for analytical purposes.
- 14.9 The Audit Manager co-ordinating RIPA and IPA applications ensures that there is an awareness of the investigations taking place. This would also serve to highlight any unauthorised **covert** surveillance being conducted.

Retention and Destruction of Material

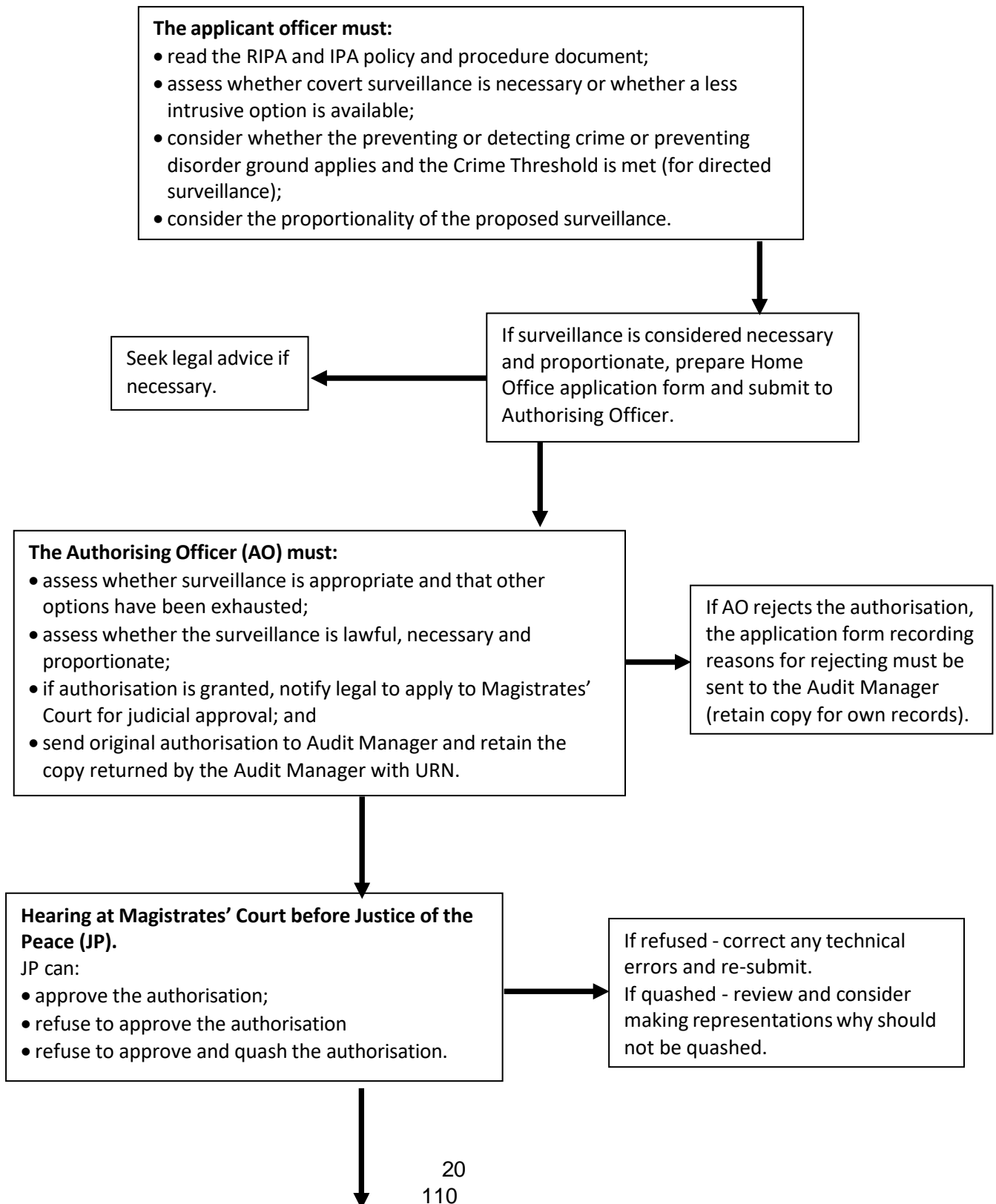
- 14.10 Departments must ensure that arrangements are in place for the handling, storage and destruction of material obtained through the use of **covert** surveillance, a CHIS and/or the acquisition of communications data which accord with the Council's Information Management Policy. Records will be reviewed after a period of 6 years from the date on which the relevant criminal or civil proceedings file is closed for archive and must be destroyed as soon as they are no longer necessary. **Confidential material must be destroyed as soon as it is no longer necessary.** It must not be retained or copied unless it is necessary for a specified purpose. Where there is doubt, advice must be sought from the Head of Legal and Support Services or the Senior Responsible Officer.

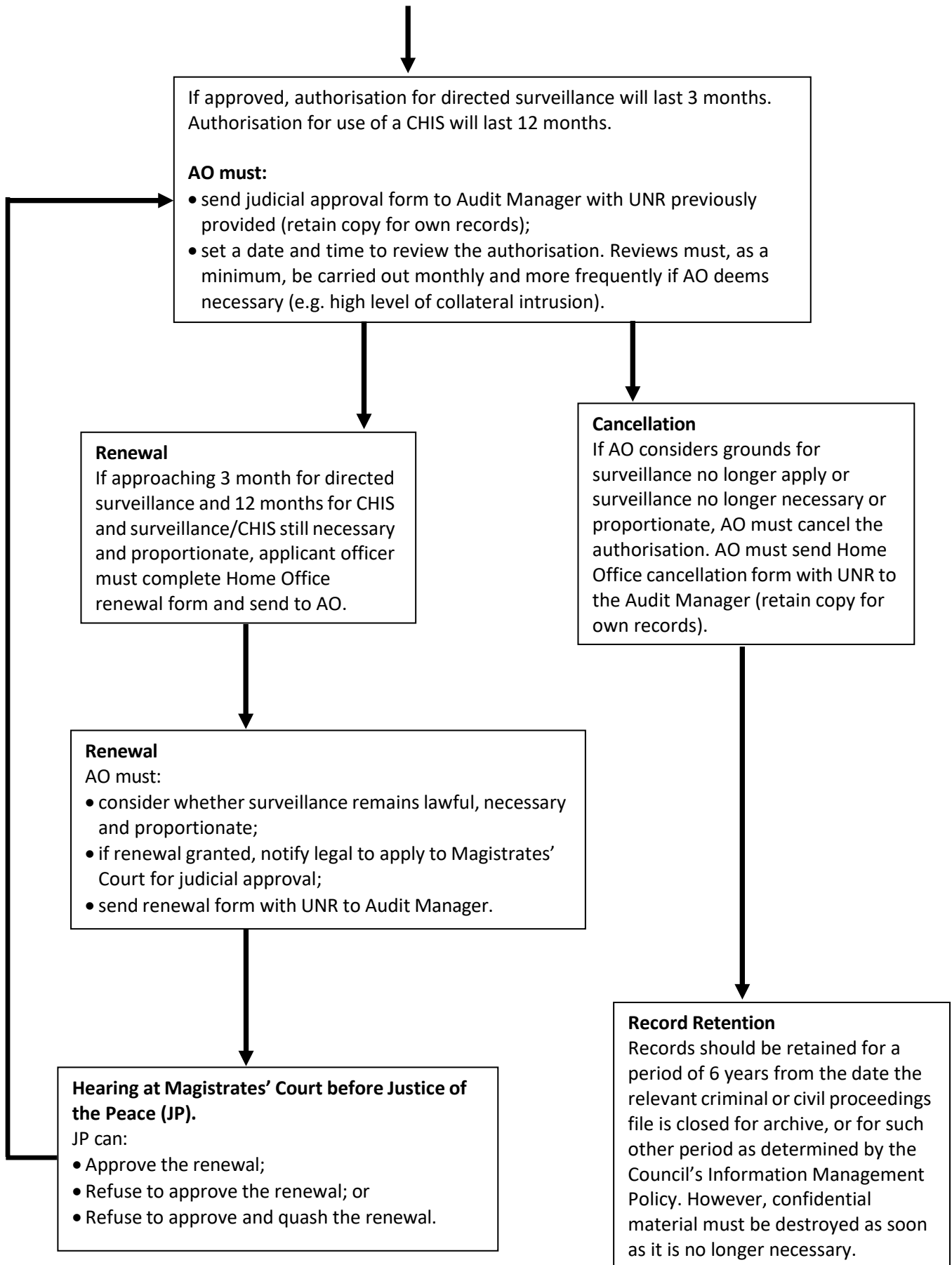
15. REVISION HISTORY

Date	Action
December 2006	ASG Revised
May 2009	ASG Reviewed
June 2010	AW Reviewed and updated
March 2012	ASG Revised
October 2012	HO Guidance issued
September 2013	RH Reviewed and updated
October 2015	DMG Reviewed and updated
9 December 2015	Approved by Audit and Governance Committee
12 January 2016	Approved by Council

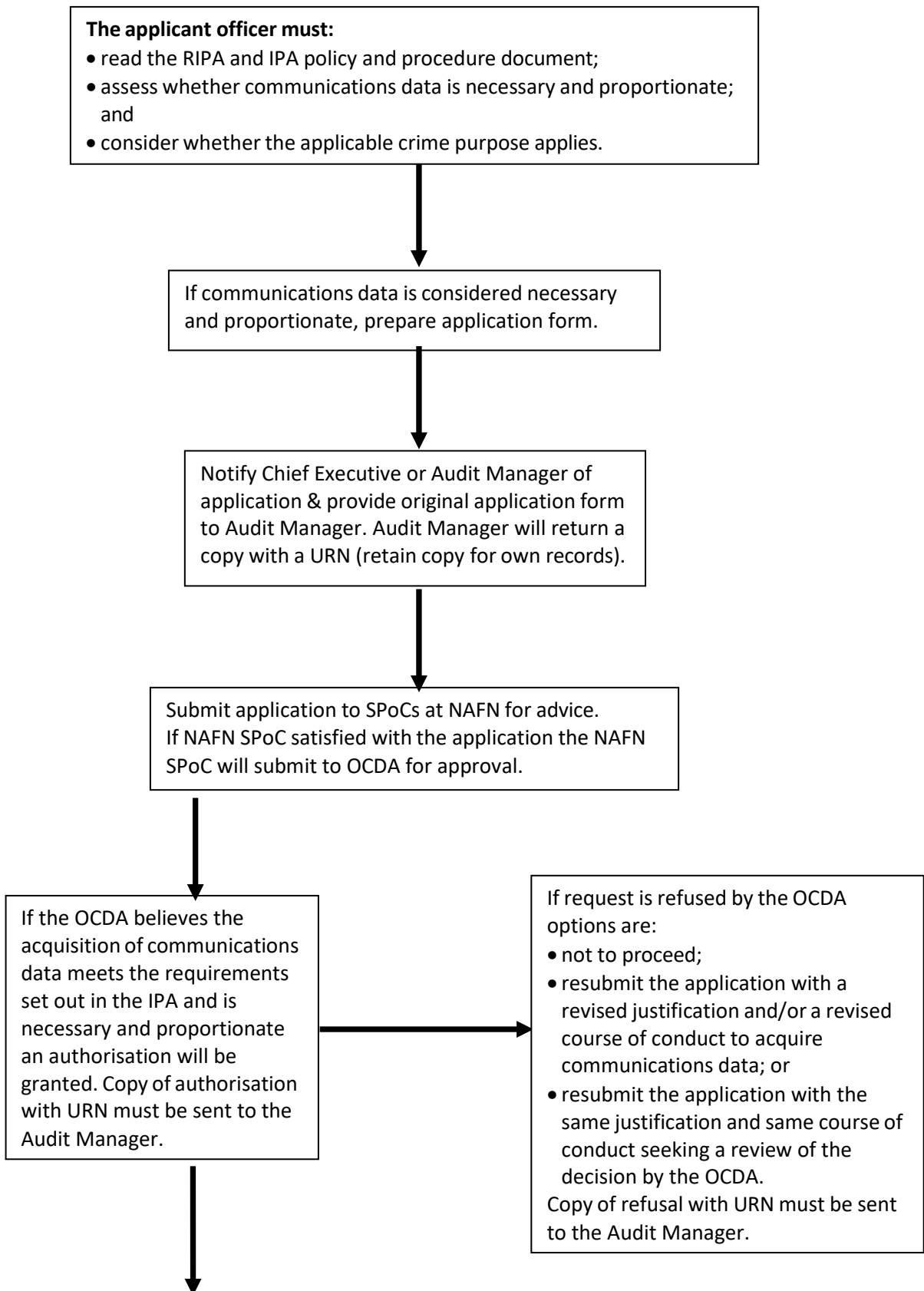
RIPA - AUTHORISATION OF DIRECTED SURVEILLANCE / USE OF A CHIS PROCEDURE

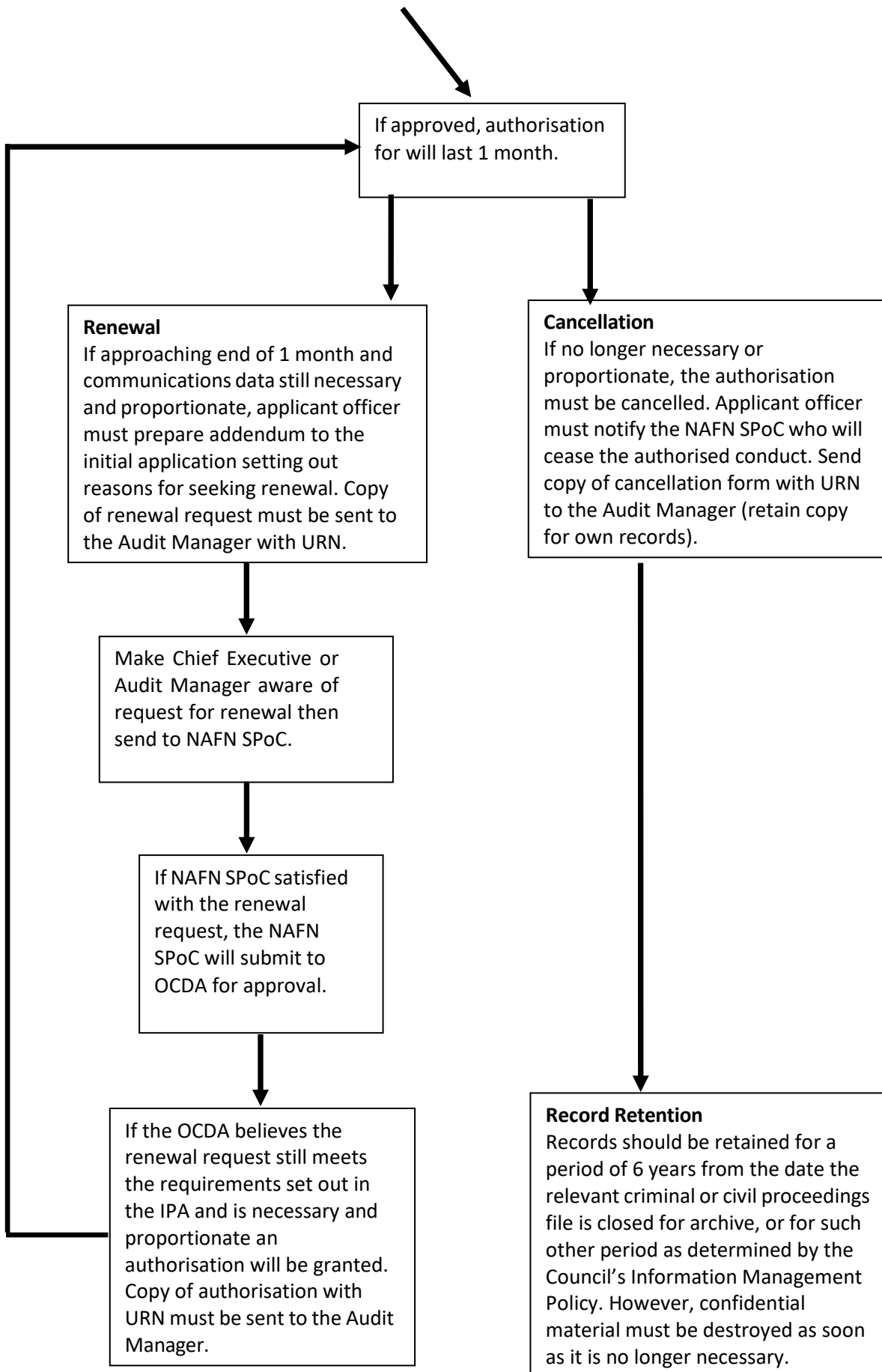
(Note: Note: Only the Chief Executive may authorise the use of a juvenile or vulnerable individual as a CHIS)





IPA - COMMUNICATIONS DATA AUTHORISATION PROCESS





This page is intentionally left blank

INFORMATION MANAGEMENT POLICY

Version No.	Author	Date	Summary of Changes
1.0	Lynn Wyeth	November 2015	Original Draft
1.1	Lynn Wyeth	December 2015	Amendments by NWLDC incorporated.
1.2	Lee Mansfield	December 2015	Amendment made following CLT decision - SIRO
1.3	Lee Mansfield	February 2016	To reference legal as location of the IM team
1.4	Sabrina Doherty	February 2017	Changes made to team structures, functions, roles and responsibilities.
1.5	Andrew Hickling/Louis Sebastian	May 2018	Changes made to team structures, functions, roles and responsibilities.
1.6	Nicola Taylor/Mackenzie Keatley	July 2020	Change made to team structures, roles and responsibilities, training and support, legislation update.
1.7	Nicola Taylor	June 2021	No changed made
1.8	Nicola Taylor	June 2022	No changes made
1.9	Laurent Flinders	May 2023	Changes made to reference UK GDPR. Changes made to the Data Protection Officer role details. Amendment made to Council address.

Version 1.9
June 2023

	Contents	Page No.
1.	Introduction	3
2.	Purpose of Policy	3
3.	Scope of this Policy	3
4.	Procedures and Guidance	4
5.	Principles of information management	4
6.	Roles and Responsibilities	5
7.	Main Themese	8
8.	Risk	9
9.	Training	9
10.	Compliance	10
11.	Fees and Charges	10
12.	Complaints	10
13.	Equalities impact Assessment	11
14.	Review of Policy	11

POLICY STATEMENT

“Information is a vital corporate asset of the Council which is of extremely high value. North West Leicestershire District Council is committed to ensuring that information is efficiently managed and that appropriate policies, procedures, management accountability and structures provide a robust governance framework for information management.”

1. INTRODUCTION

1.1 The key areas of Information Management are:

- Records Management
- Information Risk
- Information Security
- Environmental Information Regulations 2004
- Freedom of Information Act 2000
- Data Protection Act 2018
- UK General Data Protection Regulation
- Local Government Transparency Code 2015
- Privacy and Electronic Communication Regulations
- Public Services Network Code of Connection
- Payment Card Industry Security Standards
- Confidentiality

1.2 This policy is part of a set of information management policies and procedures that support the delivery of an Information Management framework, and should be read in conjunction with these associated documents, listed at section 4.

2. PURPOSE OF THE POLICY

2.1 This Information Management policy provides an overview of the Councils approach to information management, a guide to the procedures in use, and details about the management structures within the organisation.

2.2 This policy enables the Council to ensure that all information is dealt with legally, fairly, securely, efficiently, and effectively.

2.3 This policy ensures that the provisions of the Freedom of Information Act 2000 (FOI), the Environmental Information Regulations 2004 (EIRs), the Data Protection Act 2018 (DPA), the UK General Data Protection Regulation (UK GDPR) and the Public Services Network Code (PSN CoCo) are complied with.

3. SCOPE OF THIS POLICY

3.1 This policy, framework and supporting policies apply to:

- All information systems within the organisation (both electronic and paper based);
- All data, information, and records owned by the Council, but also including those held by contractors or partner organisations on behalf of, or as a result of their relationship with, the Council);
- Any information that is owned by other organisations, but may be accessed and used by Council employees;
- Information in whatever storage format and however transmitted (i.e., paper, voice, photo, video, audio or any digital format. It will also cover formats that are developed and used in the future.);
- All employees of the Council, Council members, temporary workers, volunteers, student placements etc;
- The employees of any other organisations having access to Council information, for example, auditors, contractors, and other partner agencies where there is no specific information sharing protocol in place;

3.2 The procedures outlined in this Policy are in addition to the Council's complaints procedures and other statutory reporting procedures applying to some divisions.

3.3 This Policy has been discussed with the relevant trade unions and has their support.

4. PROCEDURES AND GUIDANCE

4.1 This Information Management Policy will be strengthened by other associated Council policies/procedures/ material including but not limited to:

- ICT Security Policy;
- Request for Information Procedure;
- Security Incident Procedure;
- Records Management Procedure;
- Information Sharing Procedure;
- Whistleblowing Policy;
- RIPA Policy;
- Anti Money Laundering Policy;
- Employment Practices Code – Information Commissioner's Office;

5. PRINCIPLES OF INFORMATION MANAGEMENT

5.1 The Council understands the need for an appropriate balance between openness and confidentiality in the management and use of information. The Council also understands the need to share information with others in a controlled manner.

5.2 To maximise the value of organisational assets the Council will endeavour to ensure that data is:

- Held securely and confidentially;
- Obtained fairly and lawfully;
- Recorded accurately and reliably;
- Used effectively and ethically;
- Shared and disclosed appropriately and lawfully;

5.3 To protect the organisation's information assets from all threats, whether internal or external, deliberate or accidental, the Council will ensure:

- Information will be protected against unauthorised access;
- Confidentiality of information will be assured;
- Integrity of information will be maintained;
- Information will be supported by the highest quality data;
- Regulatory and legislative requirements will be met;
- Business continuity plans will be produced, maintained and tested;
- Information security training will be mandatory for all staff;
- All breaches of information security, actual or suspected, will be reported via the Security Incident Procedure and investigated by the Data Protection Officer or Information Management Officer;
- Significant breaches will be handled with support from Human Resources and/or ICT Manager and/or Legal Services;

6. ROLES AND RESPONSIBILITIES

6.1 Information Asset Owners

6.1.1 Information Asset Owners (IAOs) are Heads of Service who are the nominated owners for one or more identified information assets within the Council. Their role is to understand what information is held, added, removed, how information is moved and who has access and why.

6.1.2 Information Asset Owners will:

- Know what information comprises or is associated with the asset, and understand the nature and justification of information that flows to and from the asset;
- Know who has access to the asset, whether system or information, why access is required, and ensures access is monitored and compliant with policy;
- Understand and address risks to the asset, providing assurance to the Senior Information Risk Owner;
- Ensure there is a legal basis for processing data and for any disclosures made;
- Refer queries about any of the above to the Information Governance Team;

6.2 Senior Information Risk Owner

6.2.1 From 1 July 2016 the Head of Legal and Commercial Services will become the SIRO.

The SIRO will report to the CLT on all matters relating to Information Management. The SIRO is an executive who is familiar with and takes ownership of the organisation's information risk policy, and acts as advocate for information risk

6.3 Data Protection Officer

6.3.1 As of the 4 November 2018 the Council appointed a Data Protection Officer.

The DPO Information Management responsibilities include:

- Implementing information management procedures and processes for the organisation;
- Raising awareness about information management to all staff;
- Ensuring that training is provided annually and is completed by all staff;
- Coordinating the activities of any other staff given responsibilities for data protection, confidentiality, information quality, records management and Freedom of Information;
- Conducting internal audits to ensure compliance on an ad-hoc basis;
- Ensures the Council is responsible for the continued integrity of datasets and maintains and enforces applications of policies and standards;
- To cooperate with the supervisory authority (ICO).

6.4 Information Governance

6.4.1 Information Management is coordinated and managed by the Information Governance Team. The Team will:

- Assist the Senior Information Risk Owner in the implementation of their key responsibilities and any other matters as deemed appropriate and necessary;
- Maintain an awareness of information management issues within the Council;
- Review and update the information management policy in line with local and national requirements;
- Review and audit all procedures relating to this policy where appropriate on an ad-hoc basis;
- Ensure that line managers are aware of the requirements of the policy.

6.5 ICT Team Manager

6.5.1 The ICT Team Manager is responsible for:

- The formulation and implementation of ICT related policies and the creation of supporting procedures;
- Developing, implementing and managing robust ICT security arrangements in line with best industry practice, legislation, and statutory requirements;
- Effective management and security of the Council's ICT infrastructure and equipment;
- Developing and implementing a robust IT Disaster Recovery Plan;
- Ensuring that ICT security requirements for the Council are met
- Ensuring the maintenance of all firewalls, secure access servers and similar equipment are in place at all times.

6.6 Head of Service / Team Managers

6.6.1 Heads of Service / Team Managers will take responsibility for ensuring that the Information Management Policy is implemented within their team. All managers will ensure that:

- The requirements of the information management policy framework are met and its supporting policies and guidance are built into local procedures;
- There is compliance with all relevant information management policies within their area of responsibility;
- Information management issues are identified and resolved whenever there are changes to services or procedures;
- Their staff are properly supported to meet the requirements of information management and security policies and procedures, by ensuring that they are aware of:
 - The policies and procedures that apply to their work area;
 - Their responsibility for the information that they use;
 - Where to get advice on security issues and how to report suspected security incidents.

6.7 Staff

6.7.1 It is the responsibility of each employee to adhere to this policy. Staff will receive instruction and direction regarding the policy from a number of sources, including:

- Policy/strategy and procedure manuals;
- Their line manager;
- The Legal Team;
- Specific training courses;

- Other communication methods, for example, team meetings; and Staff Intranet.

6.7.2 All staff (whether permanent, temporary, voluntary or on any type of placement/training scheme) and members must make sure that they use the Council's IT systems appropriately and adhere to the relevant ICT Policies of the Council. All members of staff are responsible for:

- Ensuring that they comply with all information management policies and information security policies and procedures that are relevant to their service;
- Seeking further advice if they are uncertain how to proceed;
- Reporting suspected information security incidents.

6.7.3 Staff awareness is a key issue in achieving compliance with Information Management policies. Accordingly there will be:

- Mandatory base line training in key information management competencies for all staff;
- Additional support for all employees routinely handling 'personal data' as defined by the Data Protection Act 2018;
- All information management policies and procedures available on the intranet;
- Staff with specialist knowledge available to advise across the full range of information management areas;
- Communication and updates will be provided to staff regularly;
- Services are encouraged to have an Information Champion to represent their service. Key messages, training and support are provided to the Information Champions who feed this back to their service. Information Champions can raise issues with the group to identify and remedy problems.

7. MAIN THEMES

7.1 Openness

7.1.1 Non-confidential information which the Council hold will be made available to the public through the Councils website wherever feasible and appropriate.

7.2 Legal Compliance

7.2.1 The main legislation applying to information management is the Data Protection Act 2018 and the Freedom of Information Act 2000. The Council will establish and maintain procedures to ensure compliance with the Data Protection Act 2018, the Freedom of Information Act 2000, the Environmental Information Regulations 2004, and the Humans Rights Act 1998.

7.3 Information Security

7.3.1 Information security is concerned with the confidentiality, integrity, and availability of information in any format, and the Council must comply with the requirements of the Public Services Network.

7.4 Information and Records Management

7.4.1 To ensure that information and records are effectively managed, and that the Council can meet its information management objectives, there will be a Records Management Policy that sets out the Council's standards for handling information during each phase of the information lifecycle.

7.5 Information Quality Assurance

7.5.1 The Council will undertake or commission regular assessments and audits of its information quality and records management arrangements.

7.5.2 Managers are expected to take ownership of, and seek to improve, the quality of data within their services. Training and awareness-raising sessions appropriate to staff groups will be provided.

7.6 Partnerships and Information Sharing

7.6.1 Any sharing of personal or confidential information with partner agencies or involving individual large transfers of such information will be the subject of a written Information Sharing Agreement (ISA). This will set out the expected process, the standards of security and information handling.

8. RISK

8.1 The Council must ensure it operates within a robust information management framework to reduce the risk of threats such as potential litigation, breach of legislation, or enforcement action from the ICO for failure to respond to information requests adequately.

9. TRAINING

9.1 Appropriate training will be mandatory for all staff.

9.2. All staff will be made aware of their obligations for information management through effective communication programmes.

9.3. Each new employee will be made aware of their obligations for information management during an induction-training programme and will be required to undergo mandatory data protection training before they can pass their probation period.

9.4. Training requirements will be reviewed annually to ensure that staff are adequately trained.

10.1 COMPLIANCE

- 10.1 Failure to observe the standards set out in this policy may be regarded as serious and any breach may render an employee liable to action under the Council's Disciplinary Procedure, which may include dismissal.

11. FEES AND CHARGES

- 11.1 The Council aims to provide as much information free of charge on the website for customers to download or view at home. The Council may charge in accordance with the charges set out in legislation or statutory guidance and for the cost of disbursements such as photocopying and postage.

12. COMPLAINTS

- 12.1 Any person who is unhappy with the way in which the Council has dealt with their request for information, or how their personal data has been handled, may ask for the matter to be reviewed. All complaints should be in writing to:

- DPO@NWLeicestershire.gov.uk (personal data requests)
- FOI@NWLeicestershire.gov.uk (non-personal information request)

- Data Protection Officer
North West Leicestershire District Council
Whitwick Business Centre
Stenson Road
Coalville
Leicestershire
LE67 4JP

- 12.2 Should the requester/complainant still be unhappy with the outcome of this review they have the right to pursue their complaint to the Data Protection Officer for a formal review. Following the Internal Review, the requester can contact the Information Commissioners Office (ICO, www.ico.org.uk) by writing to:

- accessicoinformation@ico.org.uk
- Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

13. EQUALITIES IMPACT ASSESSMENT

- 13.1 Equality and diversity issues have been considered in respect of this policy and it has been assessed that a full Equality Impact Assessment is not required as there will be no adverse impact on any particular group.

14. REVIEW OF POLICY

- 14.1 This policy will be reviewed as deemed appropriate, especially in light of any legislative changes, but no less frequently than every 12 months.
- 14.2 Policy review will be undertaken by the Information Governance Team.

This page is intentionally left blank

DATA PROTECTION POLICY

Version No.	Author	Date	Summary of Changes
2.0	Nicola Taylor	June 2023	No changes

Version 2.0

June 2023

	Contents	Page No.
1.	Introduction	3
2.	What information is covered?	4
3.	Policy statement	4
4.	Principles	4
5.	Scope of this policy	5
6.	Policy	6
7.	Data protection responsibilities	6
8.	Monitoring	8
9.	Validity of this policy	8
Appendix A	GDPR 2018 – Data protection principles	9
Appendix B	Summary of relevant legislation and guidance	11
Appendix C	Rights of Data Subjects	13

1. INTRODUCTION

Background

- 1.1 North West Leicestershire District Council (NWLDC) needs to collect person-identifiable information about individuals in order to carry out its functions and fulfil its objectives. Personal data is defined as ‘information which relates to a living individual and from which they can be identified, either directly or indirectly’.
- 1.2 Personal data at NWLDC can include employees (present, past and prospective), service users, contractors and third parties, private and confidential information as well as sensitive information, whether in paper, electronic or other form.
- 1.3 Irrespective of how information is collected, recorded and processed person-identifiable information must be dealt with properly to ensure compliance with the Data Protection Act 2018 (DPA) and the General Data Protection Regulations 2018 (GDPR).
- 1.4 The DPA and the GDPR requires NWLDC to comply with the key Data Protection Principles (see Appendix A below) and to notify the Information Commissioner about the data that we hold and why we hold it. This is a formal notification and is renewed annually.
- 1.5 The DPA and the GDPR gives rights to data subjects (people that we hold information about) to access their own personal information, to have it corrected if wrong, in certain permitted circumstances to ask us to stop using it and to seek damages where we are using it improperly (see Appendix C below).
- 1.6 The lawful and correct treatment of person-identifiable information by NWLDC is paramount to the success of the organisation and to maintaining the confidence of its service users and employees. This policy will help NWLDC ensure that all person-identifiable information is handled and processed lawfully and correctly.

Data Protection and the GDPR Principles

- 1.7 NWLDC has a legal obligation to comply with all relevant legislation in respect of data protection and information / IT security. The organisation also has a duty to comply with guidance issued by the Information Commissioners Office.
- 1.8 All legislation relevant to an individual’s right to the confidentiality of their information and the ways in which that can be achieved and maintained are paramount to the Council. Significant penalties can be imposed upon the organisation or its employees for non-compliance.

- 1.9 The aim of this policy is to outline how the NWLDC meets its legal obligations in safeguarding confidentiality and adheres to information security standards. The obligations within this policy are principally based upon the requirements of the DPA and GDPR, as the key legislative and regulatory provisions governing the security of person-identifiable information.
- 1.10 Other relevant legislation and guidance referenced and to be read in conjunction with this policy, is outlined together with a brief summary at Appendix B (below).
- 1.11 GDPR requires Public Authorities to appoint a Data Protection Officer. A data protection officer (DPO) is an enterprise security leadership role required by the General Data Protection Regulation (**GDPR**). Data protection officers are responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements.

2. WHAT INFORMATION IS COVERED?

- 2.1 Personal data within the respective legislative and regulatory provisions covers 'any data that can be used to identify a living individual either directly or indirectly'. Individuals can be identified by various means including but not limited to, their address, telephone number or e-mail address. Anonymised or aggregated data is not regulated by the provisions, providing the anonymisation or aggregation of the data is irreversible.

3. POLICY STATEMENT

- 3.1 This document defines the data protection policy for NWLDC. It applies to all person-identifiable information obtained and processed by the organisation and its employees.

It sets out:

- The organisation's policy for the protection of all person-identifiable information that is processed
- The responsibilities (and best practice) for data protection
- The key principles of the DPA and the GDPR.

4. PRINCIPLES

- 4.1 The objective of this policy is to ensure the protection of information NWLDC keeps in accordance with relevant legislation, namely:

- **To ensure notification;**

Annually notify the Information Commissioner about the NWLDC's use of person-identifiable information.

- **To ensure professionalism;**

All information is obtained, held and processed in a professional manner in accordance with the provisions of the DPA 2018 and the GDPR.

- **To preserve security;**

All information is obtained, held, disclosed and disposed of in a secure manner.

- **To ensure awareness;**

Provision of appropriate training and promote awareness to inform all employees of their responsibilities.

- **Data Subject access;**

Prompt and informed responses to subject access requests.

4.2 The policy will be reviewed periodically by the NWLDC Senior Management Team. Where review and update is necessary due to legislative changes this will be done immediately.

4.3 In accordance with the council's equality and diversity policy statement, this procedure will not discriminate, either directly or indirectly, on the grounds of gender, race, colour, ethnic or national origin, sexual orientation, marital status, religion or belief, age, union membership, disability, offending background or any other personal characteristic.

5. SCOPE OF THIS POLICY

5.1 This policy will ensure that person-identifiable information is processed, handled, transferred, disclosed and disposed of lawfully. Person-identifiable information should be handled in the most secure manner by authorised staff only, on a need to know basis.

5.2 The procedures cover all person identifiable information, electronic or paper which may relate to employees, contractors and third parties about whom we hold information.

6. POLICY

6.1 NWLDC obtains and processes person-identifiable information for a variety of different purposes, including but not limited to:

- Staff records and administrative records
- Service Users records including the administering of benefits, council tax, housing records, elections, grants, planning applications, licensing applications etc.
- Matters relating to the prevention, detection and investigation of offences , fraud and corruption
- Matters relating to the enforcement of primary and secondary legislation
- Complaints and requests for information.

6.2 Such information may be kept in either computer or manual records. In processing such personal data, NWLDC will comply with the data protection principles within the DPA and GDPR.

7. DATA PROTECTION POLICIES

Overall responsibilities

7.1 The Council is the 'data controller' and permits the organisation's staff to use computers and relevant filing systems (manual records) in connection with their duties. The Council has legal responsibility for the notification process and compliance with the DPA and the GDPR.

7.2 The Council whilst retaining its legal responsibilities has delegated data protection compliance to the Data Protection Officer.

Data Protection Officer's (DPO) responsibilities

7.4 The Data Protection Officer's responsibilities include:

- Ensuring that the policy is produced and kept up to date
- Ensuring that the appropriate practice and procedures are adopted and followed by the Council.
- Provide advice and support to the Senior Management Team on data protection issues within the organisation.

- Work collaboratively with Human Resources, the Head of Law and Governance and the Compliance Team to help set the standard of data protection training for staff.
- Ensure data protection notification with the Information Commissioner's Office is reviewed, maintained and renewed annually for all use of person identifiable information.
- Ensure compliance with individual rights, including subject access requests.
- Act as a central point of contact on data protection issues within the organisation.
- Implement an effective framework for the management of data protection.
- Review Retention Schedule annually in January to ensure that it is accurate and up to date.
- Conduct department reviews to ensure that all departments are compliant and act in accordance with the retention schedule.

Line managers' responsibilities

7.5 All line managers across the Council's service areas are directly responsible for:

- Ensuring their staff are made aware of this policy and any notices.
- Ensuring their staff are aware of their data protection responsibilities.
- Ensuring their staff receive suitable data protection training.

General responsibilities

7.6 All NWLDC employees, including temporary and contract staff are subject to compliance with this policy. Under the GDPR individuals can be held personally liable for data protection breaches.

7.7 All NWLDC employees have a responsibility to inform their line manager and the Data Protection Officer of any new use of personal data, as soon as reasonably practicable after it has been identified.

- 7.8 All NWLDC employees will, on receipt of a request from an individual for information held, known as a subject access request or concerns about the processing of personal information, immediately notify the Compliance Officer.
- 7.9 Employees must follow the subject access request procedure (see Appendix C below).

8. MONITORING

- 8.1 Compliance with this policy will be monitored by the Finance and Corporate Governance team, together with internal audit reviews where necessary.
- 8.2 The Data Protection Officer is responsible for the monitoring, revision and updating of this policy document on an annual basis or sooner, should the need arise.

9. VALIDITY OF THIS POLICY

- 9.1 This policy will be reviewed at least annually by the Senior Management Team. Associated data protection standards will be subject to an ongoing development and review programme.

APPENDIX A

General Data Protection Regulation 2018 – The Data Protection Principles

1. Lawfulness, Fairness and Transparency: Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals.
2. Purpose Limitation: Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
3. Data Minimisation: Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4. Accuracy: Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
5. Storage Limitation: Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
6. Integrity and Confidentiality: Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

7. Accountability: The controller shall be responsible for, and be able to demonstrate compliance with, the previous six principles.

APPENDIX B – Summary of Relevant Legislation and Guidance

General Data Protection Regulations (GDPR)

A legal basis must be identified and documented before personal data can be processed. ‘Controllers’ and ‘Processors’ will be required to document decisions and maintain records of processing activities.

Human Rights Act 1998

This Act binds public authorities to respect and protect an individual’s human rights. This will include an individual’s right to privacy (under Article 8) and a service user’s right to expect confidentiality of their information at all times.

Article 8 of the Act provides that “everyone has the right to respect for his private and family life, his home and his correspondence”. However, this article also states “there shall be no interference by a public authority with the exercise of this right except as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention or disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others”.

Each organisation must act in a way consistent with these requirements. It must take an individual’s rights into account when sharing personal information about them.

Freedom of Information Act 2000

This Act gives individuals rights of access to information held by public authorities.

Regulation of Investigatory Powers Act 2000

This Act combines rules relating to access to protected electronic information as well as revising the “Interception of Communications Act 1985”. The aim of the Act was to modernise the legal regulation of interception of communications, in the light of the Human Rights laws and rapidly changing technology.

Crime and Disorder Act 1998

This Act introduces measures to reduce crime and disorder, including the introduction of local crime partnerships around local authority boundaries to formulate and implement strategies for reducing crime and disorder in that local area. The Act allows disclosure of person-identifiable information to the Police, Local Authorities, Probation Service or the Health Service but only if the purposes are defined within the Crime and Disorder Act. The Act does not impose a legal requirement to disclose person identifiable information and responsibility for disclosure rests with the organisation holding the information.

The Computer Misuse Act 1990

This Act makes it a criminal offence to access any part of a computer system, programs and/or data that a user is not entitled to access. NWLDC issues each employee with an individual user id and password, which will only be known to the individual and must not be divulged to other staff. This is to protect the employee from the likelihood of their inadvertently contravening this Act. NWLDC will adhere to the requirements of the Computer Misuse Act 1990, by ensuring that its staff are aware of their responsibilities regarding the misuse of computers for fraudulent activities or other personal gain. Any member of staff found to have contravened this Act will be considered to have committed a disciplinary offence and be dealt with accordingly.

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

This Act allows employers to intercept and record communications in certain prescribed circumstances for legitimate monitoring, without obtaining the consent of the parties to the communication.

APPENDIX C – Individual Rights of the Data Subject

1. The Right to be Informed: Individuals have the right to be provided with clear and concise information about what an organisation does with their personal data. NWLDC has published Privacy Notices for each of its departments that outline in detail what data we collect, how that data is used, the lawful basis for processing the data and for how long we will retain that data. These can be found on our website at:
https://www.nwleics.gov.uk/pages/data_protection_notice.
2. The Right of Access: Individuals have the right to access their personal data that is held by an organisation (commonly referred to as Subject Access). You have the right to obtain a copy of your personal data by making a Subject Access Request as detailed below.
3. The Right to Rectification: Individuals have the right to have inaccurate personal data rectified, or completed if it is incomplete. You can make a request for rectification as detailed below.
4. The Right to Erasure: Individuals have the right to have their personal data erased or 'forgotten' in certain circumstances. These include when the data is no longer necessary for the purpose in which we originally collected or processed it, when we are relying on your consent to process the data and you choose to withdraw that consent, when we are relying on legitimate interests as our basis for processing and you object to this processing (so long as there is no overriding legitimate interest to continue this processing), we have processed the personal data unlawfully, we have to do it to comply with a legal obligation or we have processed the personal data to offer information society services to a child. The Right to Erasure is not an absolute right and only applies in these circumstances listed; however, we will make every effort to assist you. You can make a request for erasure as detailed below.
5. The Right to Restrict Processing: Individuals have the right to restrict or suppress the processing of their personal data where they have a particular reason for wanting the restriction. This is not an absolute right and only applies in certain circumstances. When processing is restricted, we are permitted to store the data, but not to use it. This right may apply if you are contesting the accuracy of your data and we are verifying that accuracy, if the data has been unlawfully processed and rather than invoking the Right to Erasure you request restriction instead, if we no longer need the personal data but you need NWLDC to keep it in order to establish, exercise or defend

a legal claim, or you object to our processing of your data and we are considering whether our legitimate grounds for processing override your request. You can request the restriction of data processing as detailed below.

6. The Right to Data Portability: Individuals have the right to obtain and reuse their personal data for their own purposes across different services. This allows you to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability. You have the right to request that we transfer the data you have provided to NWLDC directly to another Data Controller. This right only applies when the lawful basis for processing the information is consent or for the performance of a contract and we are carrying out the processing by automated means (in other words, it excludes paper files). You can make a data portability request as detailed below.

7. The Right to Object: Individuals have the right to object to the processing of their data in certain circumstances. You have the absolute right to stop your data being used for direct marketing. You may also object to processing if it is for a task carried out in the public interest, the exercise of official authority vested in us or our legitimate interests (or those of a third party); however, the right to object is not absolute in these circumstances. You can make an objection as detailed below.

8. Rights in Relation to Automated Decision Making and Profiling: The GDPR has provisions on making a decision solely by automated means without any human involvement and the automated processing of personal data to evaluate certain things about an individual. All automated decision-making and profiling is subject to the GDPR and NWLDC will identify, when applicable, whether any of our data processing relies solely on automated decision-making or whether we use profiling of any kind. This information is available on our website at https://www.nwleics.gov.uk/pages/data_protection_notice

To invoke these rights, simply submit your request to us in writing either by email at dpo@nwleicestershire.gov.uk or to:

North West Leicestershire District Council
Council Offices
Whitwick Road
Coalville
Leicestershire
LE67 3FJ

For all requests, NWLDC will have one calendar month in which to respond.

VERSION CONTROL			
Version	Date Issued	Author	Update Information
V1.0	21/05/18	B. Wilson	Original approved version.
V2.0	28/01/2019	N. Taylor	Amended to reflect updated policy.

Version Awareness

The audience of this document should be aware that a physical copy may not be the latest available version. The latest version, which supersedes all previous versions, is available on our website. Those to whom this policy applies are responsible for familiarising themselves periodically with the latest version and for complying with policy requirements at all times.

DOCUMENT CONTROL	
Prepared By	Data Protection Officer
Original Authorisation By	Senior Management Team
Review Period	One year
Classification	Public

This page is intentionally left blank

ICT AND CYBER SECURITY POLICY SEPTEMBER 2023

Version No.	Author	Date	Summary of Changes
2.5	Sam Utama	June 2023	No Changes
2.5	Sam Utama	September 2022	Update to include Internet and Email security form
2.4	Sam Utama	April 2021	Update to section 5.2
2.3	Sam Utama	June 2020	General review and update
2.2	Sam Utama	May 2019	Update to Cyber Security
2.1	Sam Utama	September 2017	Update Password Control
2	Sam Utama	July 2017	General Update
1.1	Ivan Arkininstall	July 2013	Revised
1	Phil Clarke	March 2009	Revised

**Version 2.5
June 2023**

	Contents	Page No.
	Foreword	5
	Policy Objectives	5
	Scope	6
1.	Security Organisation	7
1.1	Responsibilities	7
1.2	Acquisition of Information Systems and Technology	8
1.3	Security Information Advice	8
1.4	Security Incidents	8
1.5	Independent Review of Information Security	9
2.	Security of Third Party Access	9
2.1	Identification of Risks from Third Party Access	9
3.	Asset Control	10
3.1	Inventory of Assets	10
4.	Personnel Security	10
4.1	General	10
4.2	ICT Security Training	11
4.3	Responding to Incidents	12
5.	Physical and Environmental Security	12
5.1	Secure Areas	12
5.2	Equipment Security	13
5.3	Equipment and Data Destruction	14
5.4	Remote Access to Systems and Data	14
6.	Computer and Network Management	15

6.1	Operational Procedures and Responsibilities	15
6.2	System Planning and Acceptance	15
6.3	Configuration and Change Management	16
6.4	Protection from Malicious and Unauthorised Software	16
6.5	Housekeeping	17
6.6	Network Management	18
6.7	Media Handling and Security	18
6.8	Data and Software Exchange	19
6.9	Connection to Other Networks	20
6.10	Electronic Mail	20
6.10.1	Confidential or RESTRICTED Information	21
6.10.2	Use of E-mail Outside the UK	21
6.11	Internet	21
7.	System Access Control	23
7.1	Business Requirement for System Access	23
7.2	User Access Management	23
7.3	User Responsibilities	24
7.4	Network Access Control	24
7.5	Computer and Application Access Control	25
8.	Systems Development and Maintenance	25
8.1	Security Requirements in Systems	25
8.2	Security of Application System Files	26
8.3	Security in Development and Support Environments	26
9.	Compliance	27

9.1	Compliance with Legal Requirements and Codes of Practice	27
9.1.1	Control of Proprietary Software Copying	27
9.1.2	Use of Unlicensed Software	28
9.1.3	Safeguarding of the Council's Records	28
9.1.4	Auditing and Logging the use of ICT Resources	28
9.1.5	Data Protection	28
9.1.6	Prevention of Misuse of ICT Facilities	29
9.2	Security Review of ICT Systems	30
9.3	System Audit Considerations	30
	Appendices	
	Appendix 1 - The National Protective marking Scheme	31
	The PROTECT Classification	32
	The RESTRICTED Classification	33
	Major Differences Between PROTECT and RESTRICTED	34
	Appendix 2 – Internet and Email conditions of use	35
	Appendix 3 - GCSx Personal Commitment Statement	41
	Appendix 4 - Third Party Code of Connection	45

ICT AND CYBER SECURITY POLICY

FORWARD

North West Leicestershire District Council is dependent upon its Information and Communications Technology (ICT) systems for its normal day to day business activities. It is therefore essential for the continued successful operation of the Council that the confidentiality, integrity and availability of its ICT systems and data are maintained at a high level at all times. There is also an obligation on the Council and all employees to comply with relevant legislation such as the General Data Protection (GDPR) Acts, the Copyright, Designs and Patents Act and the Misuse of Computers Act.

The majority of information used by the Council is now available and kept in an electronic format and this policy is centred on the need to ensure that our technology and IT systems are sufficiently secure to protect the underlying information and suitably protected. This does, however, need to be backed by a wider culture of confidentiality and security of information in any form including direct conversations, telephone conversations and the written word.

It follows that the highest standard of IT security is required within the Council. To achieve this, the ICT Security and Cyber Security Policy has been introduced and everyone who uses IT equipment is expected to read it and ensure that its provisions are complied with. There is also a short summary of this policy containing the main aspects affecting the average user.

The key to ensuring that the Council's data and systems remain secure is to ensure that all staff are aware of their own responsibilities they will be required to:

- acknowledge receipt and understanding of this policy document;
- in the case of staff having access to RESTRICTED data via the Government Connect Secure Extranet (GCSx) or Government Secure Intranet (GSi) will agree to abide by specific ICT security rules regarding such information (see Appendix 2).

Wilful failure to follow the procedures stated in this policy may lead to disciplinary action, prosecution and may also render the person personally liable for the cost of replacing or reinstating damaged or corrupt equipment and data.

The policy will be reviewed periodically (at least annually) and updated by the ICT Manager. If you have any doubts about the meaning of any part of this policy, or believe that it could be improved in any way, please contact the ICT Manager.

POLICY OBJECTIVES

This policy also sets out the overall objective and principles underlying ICT and cyber security at North West Leicestershire District Council and specifies the management arrangements and key responsibilities.

The objective of this ICT and Cyber Security Policy and its supporting policies is to ensure the highest standards are maintained across the Council at all times so that:

- (a) the public and all users of the Council's information are confident of the confidentiality, integrity and availability of the information used and produced.
- (b) Business damage and interruption caused by cyber security incidents are minimised.

- (c) All legislative and regulatory requirements are met.
- (d) The Council's information is used responsibly, securely and with integrity at all times and that this applies to manual and electronic information.

The main objectives of this policy are:

- to ensure adequate protection of all the Council's assets, locations, people, programs, data and equipment, on a cost-effective basis, against any threat which may affect their security, integrity and/or the level of IT service required by the Council to conduct its business;
- to ensure awareness amongst the Council's officers and members of all relevant legislation and that they fully comply with such legislation;
- to ensure awareness within the Council of the need for IT and cyber security to be an integral part of the day to day operation of the Council's business;
- to ensure user security awareness training is in place and all staff have access to that training.

The strategic approach to cyber security is based on:

- consistency of approach with the implementation of key processes and procedures
- the application of recognised security management good practice such as the Cyber Essentials PLUS and ISO/IEC 27000 family of information management systems standards;
- implementation of physical, personal, procedural and technical counter and mitigation measures;
- annual cyber security assessments and risk mitigations of external and internal threats, commonly called ICT security penetration test carried out by a third party CREST/IASME accredited supplier;
- the continuing availability of specialist security advice;
- cyber security is a vital area of concern, with ever increasing threat vector, that will receive the regular attention of senior management, through the risk and management committee and the Corporate Leadership team;
- all users have an essential role to play in maintaining sound IT and cyber security and will be fully supported by attending QTRLY user awareness security training;
- yearly IT audits conducted by an external supplier, to provide assurance on key ICT controls.

SCOPE

This Information Technology and Cyber Security Policy will apply to:

- all the Council's employees, members, contractors, partners and agents;
- all assets owned by the Council;
- information held or owned by North West Leicestershire District Council, any ICT equipment and infrastructure used, and the physical environment in which the information and/or supporting ICT is used;
- all members of the Council who use the Council's ICT facilities;
- employees and agents of other organisations who directly or indirectly support the Council's IT services;
- members of the public using IT resources to access data on Council premises;
- Council's systems in a hosted / cloud environment.

Where access is to be granted to any third party (e.g. contractors, service providers, voluntary agencies, and partners) compliance with this policy must be agreed and documented, following the third party code of connections policy in Appendix 3. A copy of this policy and the summary document will be issued to all the above.

1. SECURITY ORGANISATION

Objective:

To manage information and cyber security within North West Leicestershire District Council to the highest level.

1.1 Responsibilities

The ICT Manager is responsible for:

- assigning security roles and responsibilities;
- co-ordinating the implementation of the security policy across the Council;
- reviewing and if appropriate updating the Security Policy;
- reviewing and monitoring security incidents;
- reviewing third party access and security arrangements;
- monitoring exposure to major threats to information assets;
- agreeing and supporting Council-wide security initiatives;
- ensuring patch management of devices is performed on a monthly basis and monitored.

The security of all hardware situated in departments and sections is the responsibility of the departmental or service manager.

The security of all other hardware, operating systems, PC application, networking, infrastructure and corporate software is the responsibility of the ICT Manager.

Departmental application software is the responsibility of:

Application	System Administrator	System and Data Owner
General Ledger	Financial Planning	Head of Finance
Creditors and Debtors	Exchequer Services	Head of Finance
Payroll	HR	Head of HR and Organisation Development
Revenues and Benefits	Partnership	Head of Customer Services
Housing Management	Strategic Housing	Head of Housing
Housing repairs	Strategic Housing	Head of Housing
Cash Receipting	Exchequer services	Head of Finance
Planning, Building Control	ICT	Head of Planning and Regeneration

Geographic Information System	ICT	Head of Planning and Regeneration
Environmental Health and Licensing	ICT	Head of Community Services
Electoral Registration and Elections	Elections Officer	Head of Legal and Commercial Services
Personnel	HR and Organisation Development	Head of HR and Organisation Development
Land Charges	ICT	Head of Planning Services and Regeneration
Electronic Document Management	ICT	Head of Planning services and Regeneration
Leisure Services Bookings	Business Development manager (Leisure)	Head of Community Services

1.2 Acquisition of Information and Communications Technology

All acquisitions of Information and Communications Technology (ICT) shall be in accordance with Council Procurement Procedures and be co-ordinated by the ICT Manager who shall obtain specialist advice if he considers it appropriate.

All new acquisitions of a corporate nature shall be agreed by the Corporate Leadership Team.

Departmental acquisitions shall be agreed between the appropriate Head of Service and the ICT Manager.

The ICT Manager has delegated authority to replace obsolete equipment in accordance with an agreed replacement program and to upgrade/replace office productivity tools and software within an agreed programme.

All new projects will be in accordance with the Council's corporate project management policies, have associated business case / justification documents and be in accordance with the current ICT strategy / road map.

1.3 Security Information Advice

Specialist advice on information security is available internally from the ICT Manager or Internal Audit.

1.4 Security Incidents

All suspected and actual security incidents shall be reported immediately to the ICT Service desk. Each incident will be recorded, investigated and corrective action implemented where appropriate. If the incident is perceived to be of a serious or urgent nature it will be escalated to the ICT manager or the Head of Customer Services.

The Council has a separate ICT Security Incident Reporting Procedure which gives full details on how to report any security incidents and this includes a copy of the reporting form which you may be asked to complete by the ICT Service desk.

This document is available from within the IT section of the Council Intranet

1.5 Independent Review of Information Security

The content, implementation and practice of this policy will be reviewed independently to provide assurance that organisation practices properly reflect the policy and that the policy is feasible and effective. Independent reviews will be carried out by the internal Audit team and External Auditors (KPMG) or one that has been appointed.

2. **SECURITY OF THIRD PARTY ACCESS**

Objective:

To maintain the security of organisational ICT facilities and information assets accessed by third parties. Either on premise or hosted environment.

2.1 Identification of Risks from Third Party Connections

Where there is a business need for third party access to ICT facilities and information assets the security implications and requirements will be determined, and controls agreed with the third party.

All new systems will be assessed for risks from third party connections and, where appropriate, controls will be defined in a contract with the third party, as described in Appendix 3.

Arrangements involving third party access, e.g. Support engineers, subcontractors, consultants will be based on a formal contract or security agreement containing, or referring to, all of the necessary security conditions to ensure compliance with the Council's security policy including obtaining an indemnity in respect of any loss caused by erasure or alteration of data or incorrect alteration of programs. The contract should be in place before access to the ICT facilities is provided.

See Appendix 3 for sample security agreement for use by third parties.

The implementation of any changes to systems should be strictly controlled using formal change control procedures. Any third party organisation carrying out work for the Council will be expected to comply with these change control procedures and will ensure that all system changes are documented. The ICT change control policy is available via the ICT intranet page.

All third party access will be controlled and is available to service providers via a secure internet connection using an SSL (secured sockets layer) VPN appliance, or an application such as Team Viewer.

Where reasonably possible, for all access will use multi factor authentication using a soft token delivered via SMS to the user's mobile phone or a mobile app. The remote support user will be given an access code and a onetime use password for that session.

All systems have passwords enabled to ensure only authorised parties can access the Council's ICT, at agreed times and that each third party can only access the relevant systems.

All contractors, consultants or other temporary staff will be issued with a unique user code and password in line with current procedures for the particular system being used. **Under no circumstances should Council staff allow their own user code or password to be used by anyone else.**

In certain circumstances it may be necessary to divulge a password for access by technical support staff and in such cases, it must be changed immediately after the authorised activities are completed. A log of such activity is maintained by the ICT department.

A log of all third party access will be recorded on the Service Desk management system, with a copy of the completed third party access control form. All third parties accessing Council systems or data must have had their own IT Security tested by a trusted third party or hold a valid accreditation such as Cyber Essentials or ISO 27001.

3. ASSETS CONTROL

Objective:

To maintain appropriate protection of organisational assets:

3.1 Inventory of Assets

An inventory of ICT assets shall be maintained by the ICT Manager who shall promptly update it for all acquisitions, disposals, updates and management of our cyber assets (this include transfer of assets to another user).The accuracy of the inventory shall be verified annually in accordance with Financial Procedure Rules. This includes equipment at staff homes for those who are working in an agile manner.

All users must notify ICT if they move an asset to another location, within the Council Offices or a remote site.

4. PERSONNEL SECURITY

Objective:

To reduce the risks of human error, theft, fraud or misuse of facilities:

4.1 General

Security roles and responsibilities for all staff using ICT facilities will be included in job descriptions and contracts where appropriate by the relevant manager. Managers are responsible for ensuring job descriptions or codes of conduct address all relevant security responsibilities.

All potential recruits will be screened by:

- obtaining two satisfactory references;
- confirming academic and professional qualifications.

All employees and third party users of ICT facilities will be required to sign a confidentiality (non-disclosure) undertaking. Revenue Services benefits staff will be subject to recruitment procedures included in the Benefits Anti-Fraud Strategy.

The appointment of employees with access to information classified as PROTECT or RESTRICTED (see Appendix 1) will be subject to the specific Baseline Personnel Security Standards available on request from the Human Resources department.

All users are responsible for the equipment issued to them and information that they have access to. Third party access to ICT equipment and data, without prior arrangement with IT is prohibited. When accessing Council information, they must ensure that they do so in a secure environment and that persons who are not authorised to view said information cannot view it.

4.2 ICT and Cyber Security Training

Objective:

To ensure that users are aware of information security and cyber threats and concerns, and are equipped to comply with and support the Council's security policy in the course of their work:

All users will need to undertake a cyber security user awareness e-learning training module.

All ICT users will be briefed in security procedures and the correct use of ICT facilities by IT staff in order to minimise possible security risks to the confidentiality, integrity and availability of data or services through user error. Managers are responsible for ensuring such training is provided to their staff.

New user accounts will only be established and issued to staff who have received appropriate ICT induction and have been authorised by the relevant Head of Service or Director. All new ICT users will be issued with either a paper copy of the current ICT and Cyber Security Policy or given access to the document on the Council's intranet. They must read the document and sign to acknowledge the terms and conditions within 2 working weeks otherwise network access will be denied.

All new ICT users who will have access to the Government Connect Secure Extranet (GCSx) or Government Secure Internet (GSi) networks will be also be required to comply with a Personal Commitment Statement pertaining to those services.

Access levels to review / amend / delete data will be determined by the relevant Head of Service in association with the system owner(s) of any ICT applications which the new user intends to use.

All third party suppliers, contractors and temporary staff will be required to read and acknowledge the terms and conditions before being granted access to Council ICT resources.

In the case of third party support companies where individual users may not be easily identifiable a board level representative of the company will be required to acknowledge the terms and conditions.

4.3 Responding to Incidents

Objective:

To minimise the damage from security incidents and malfunctions, and to monitor, learn from and reinforce procedures in the light of such incidents:

A security incident shall mean:

- any event arising from negligence or deliberate default that has, or could have, resulted in loss or damage to the Council's IT systems or data;
- a compromise to the confidentiality, integrity or availability of IT systems or data;
- an action that is in breach of the security policy;
- any cyber security threat or incident.

All security incidents shall be reported immediately to the ICT Service Desk who will pass the calls to the ICT Security Officer or ICT Manager who will instigate an investigation and report any incidents that cause serious loss or damage to the Head of Customer services and the Data protection officer. Any security incident that may have the potential to lead to disciplinary action will involve the appropriate involvement and consultation with the Head of Human Resources and Organisation Development and/or (depending upon the nature of the incident) the Audit Services Manager.

The Council has a separate ICT Security Incident Reporting Procedure which gives full details on how to report any incidents and this includes a copy of the reporting form which you may be asked to complete by the ICT Service desk. This document is available from within the IT section of the Council Intranet. The security incident will also be logged on the ICT Service Desk system.

Any security incident which leads to loss or damage, or wilful abuse of the conditions of this policy may be cause for investigation and, where appropriate, formal action, in accordance with the Council's agreed disciplinary policy.

Any incident or suspected incident must be handled in the manner as laid out in the Council's Incident and Response Policy and Procedures. The above Incident Response Policy and Procedures will be reviewed on a yearly basis.

5. **PHYSICAL AND ENVIRONMENTAL SECURITY**

Objective:

To prevent unauthorised access, damage and interference to ICT services to prevent loss, damage or compromise to assets and to the confidentiality, integrity or availability of IT systems or data, and interruption to business activities:

5.1 Secure Areas

ICT facilities such as servers, server rooms and hosting facilities, hubs and routers supporting critical or sensitive business activities shall be housed in secure areas, i.e. protected from unauthorised access, damage and interference.

Except for systems specifically intended for public use, ICT facilities should only be available to authorised persons, and wherever possible should be kept away from

public access, and preferably view. Specialised IT equipment should be further restricted to authorised staff only in areas of extra security.

The following specific conditions will apply to such secure areas:

- server rooms will be protected by electronic locking systems or digital locks on all entry points and will always be kept locked;
- access to any hosted / Data Centre facility is only for NWLDC ICT staff, with proof of identification and access granted via a request system or logging portal;
- access to server rooms will be only to ICT support staff or to others acting under their close supervision;
- server rooms will be protected with fire detection and control equipment (FM200 Gas). Such equipment will be integrated into the Council's overall fire detection system;
- servers will be protected by Uninterruptible Power Supplies (UPS) enough to allow continuous working of equipment for a minimum of 2 hours in the event of loss of electrical supply to the rooms;
- server rooms will be regularly monitored to ensure an adequate operating environment for the equipment contained;
- network distribution cabinets will be protected with UPS enough to allow continuous working for a minimum of one hour;
- network distribution cabinets will always be kept locked and access granted only to ICT network support staff or others acting under their close supervision;
- remote access may be allowed to server, network and telephony equipment but will be limited to ICT support staff and specified third party support organisations. (Access by third parties will be subject to agreements specific to the software / equipment concerned and, always, will be with the express permission of ICT staff). This includes completing the Permit to work and Risk assessment documents, for all external contractors requiring access to the server room;
- A complete log of remote access by third party support organisations will be maintained.

5.2 Equipment Security

ICT equipment and cabling should be protected from spillage or leaks and must be sited away from where staff or the public walk and also to minimise opportunities for unauthorised access or removal. Staff should also be warned of the dangers of spilling liquids or food on IT equipment. **Except for laptop and portable computers only IT staff should move, or supervise the moving, of IT equipment.**

All critical ICT equipment shall be protected by an uninterruptible power supply (UPS). UPS equipment should be self-testing and shall also be manually tested by IT staff at least every six weeks and serviced as necessary.

Officers and members should always ensure that computer equipment and screens are positioned to prevent unauthorised viewing of data.

Any faulty ICT equipment shall be reported to the IT section who will arrange for its repair or replacement. **Under no circumstances shall members of staff attempt to repair, move, change equipment or open casings except for printers to replace consumables or clear a paper jam.**

Computers provided by the Council for use at home are for the sole use of that officer or member, no unauthorised third party is allowed access to the computer equipment

for any reason. **The officer or member will be responsible for ensuring that computer is, always, used in accordance with Council conditions of use.**

Laptop, portable computers and smart phones (unless permanently assigned to an officer or member) may be borrowed, with the permission of the officer's manager, from the IT section who will maintain a record of issue and returns. Such equipment must be transported in appropriate carrying cases, such equipment must be transported in appropriate carrying cases and must not be left in clear view. If left in a vehicle it **MUST** be out of sight. **Officers should treat laptop, smart phones and portable computers as if it were their own possession and uninsured.**

Any laptops, smart phones or computers currently assigned on a permanent basis to an officer or member can be recalled for a software audit on a one-week notice. The officer or member must arrange a mutually convenient time when the computer can be returned to the IT department within that week period. Once the audit has been conducted the IT department will either return the computer or inform the officer or member and arrange a collection time and date.

5.3 Equipment and Data Destruction

Obsolete equipment shall be checked by IT staff and all hard disks will be thoroughly cleansed of data before disposal, whether by sale, donation or destruction. Equipment will normally be disposed of via a third party accredited data disposal organisation who will ensure recycling, where possible. Any PCs disposed of by sale / donation will not include the operating system installed and no application software.

All ICT equipment will be disposed of in accordance with the relevant environmental legislation e.g. WEEE Directives.

A separate procedure document "Managing, Tracking and disposing of ICT assets", is available on the ICT intranet page.

5.4 Remote Access to Systems and Data

Where there is a business need, the Council will allow employees and members to have remote access to data and systems from locations not covered by the Council local and wide area networks. This will include 'roaming' users who with suitable technology are able to access data anywhere and 'fixed point' users such as home workers. Access to systems from non-council devices, will be controlled via multi factor authentication.

The Council will allow such remote users to make use of their own PC equipment subject to meeting minimum security standards including having up to date anti-virus and firewall software.

Remote access to Council systems will only be granted on the Authority of the relevant Head of Service or Director

Remote access will be only available by using multi factor authentication (i.e. the use of a 2 part password). NWLDC operates soft tokens which require the use of a unique personal PIN either sent to the work mobile combination with a dynamically generated pass code or generated with a mobile app.

Specific conditions and responsibilities will apply to those users:

- data must not be stored on non-Council devices used for remote access;
- confidential data must be encrypted on storage devices supplied by the ICT department;
- particular care should be taken with removable storage devices such as USB sticks, etc and if these are used to move or transfer data it must be stored in encrypted format using supplied "Safe Sticks";
- any Council data downloaded or stored on employees' remote users' PC equipment must be kept secure and inaccessible to others. Data must be removed as soon as is practicable when it is no longer required;
- any loss of equipment (own or Council) must be reported immediately to the ICT Service Desk;
- any actual or perceived security threat relating to remote use of Council IT systems must be reported immediately to the ICT Service Desk;
- no RESTRICTED information should ever be used on employees / members own equipment.

When undertaking video or conference calls discussing or displaying Council information, they must ensure that no unauthorised person are privy to that information.

6. COMPUTER AND NETWORK MANAGEMENT

6.1 Operational Procedures and Responsibilities

Objective:

To ensure the correct and secure operation of computer and network facilities:

The ICT Manager is responsible for the management and operation of all servers and networks and associated specialised hardware. Departmental managers are responsible for the safe day to day operation of portable and desktop computers and printers issued to them or their staff.

Appropriate documented procedures for the management and operation of all servers and networks will be established by computer staff.

Clearly documented procedures shall be prepared by computer staff and/or the system administrator for all operational computer systems to ensure their correct, secure operation.

6.2 System Planning and Acceptance

Objective:

To minimise the risk of systems failure:

Advance planning and preparation are required to ensure the availability of adequate capacity and resources.

Acceptance procedures for new systems will include the following:

- performance and computer capacity;
- preparation of error recovery and restart procedures;

- preparation and testing of routine operating procedures;
- evidence that the new system will not adversely affect existing systems, particularly at peak processing times;
- training in the operation or use of new systems;
- formal consideration of the need for ongoing maintenance and support by a third party.

Emergency fall back arrangements should be identified for each system and adequate fall-back arrangements made wherever possible. Fall back arrangements for each system should be fully documented and responsibility for this lies with the relevant system administrator.

6.3 Configuration and Change Management

Objective:

To document and manage the ICT structure and any changes thereto:

Operational changes must be controlled to reduce the risk of system or security failures. The ICT Manager is responsible for ensuring that changes to software or hardware are carried out in a controlled manner and appropriately documented.

A formal change control (and authorisation) is in place which requires significant changes to software and hardware to be assessed, tested and verified before completion. This procedure will apply to anyone making such changes including permanent staff, temporary and contract staff, suppliers and third party support organisations.

All PCs and servers are configured and installed with a standard security configuration, which may be changed only on the authority of the ICT Manager. Any attempts to amend the standard configuration will be logged and monitored.

Specific protective measures are applied to servers accessed by users outside the Council's main network. Such servers are in a separate secure zone of the network known as a de-militarised zone or DMZ.

Please refer to "ICT Server Build Policy" and "ICT PC Build Policy" for full details.

Changes to software and hardware will, wherever possible, be applied in a test environment before being applied to operational systems.

6.4 Protection from Malicious and Unauthorised Software

Objective:

To safeguard the integrity of software and data:

It is essential that special measures, as detailed below, are implemented to prevent the introduction of malicious software such as computer viruses, ransomware and malware or the use of unauthorised software. Using unlicensed software can result in a raid (authorised by the courts) to identify the use of such unlicensed software which can result in a fine, adverse publicity and a block on the use of ANY computers until the licences are paid for or the offending software is removed, resulting in very serious disruption to the organisation's activities.

In extreme cases staff could face imprisonment. A computer virus or similar can cause severe damage to data and hence serious disruption. Every precaution must be taken to protect Council data and programs.

Unauthorised software is software that has not been purchased by, or whose purchase or use has not been agreed by the ICT Manager.

To reduce the risks of infection or use of unauthorised software the following preventive, detective and corrective measures will be instituted:

- **the introduction and/or use of unauthorised software, including screensavers, is prohibited and may lead to the application of relevant, formal disciplinary action;**
- software licences will be complied with at all times;
- Reputable, up to date anti-virus software will be used to detect and remove or isolate viruses and malware;
- **staff or members must not transfer data from their home PC to the Council computers, whether by removable storage media or e-mail, unless their home PC has up to date (i.e. definitions updated within the previous week) anti-virus software and firewall installed. The anti-virus software used must be one verified by the Council's ICT support staff;**
- **removable storage media devices are blocked from being connected to corporate devices;**
- any suspected viruses must be reported immediately to the computer section and, where appropriate, logged as a security incident;
- except where there is a justifiable business reason that has been expressly agreed with the ICT Manager, users should not open unsolicited e-mails from unverifiable sources and especially any attachments as there is a significant risk, they may contain a virus;
- **users must not attempt to download executable files, i.e. program software, from the Internet without prior specific clearance from IT staff;**
- any incoming e-mail that contains executable or compressed attachments will be automatically quarantined and routed to IT staff for checking before delivery to the intended recipient.

USB devices and removable media are not allowed on any machine. Device management software is in place to detect and block this type of activity. ICT can provide encrypted USB "safe sticks" for transfer of data, which is prohibited on all machines.

6.5 Housekeeping

Objective:

To maintain the integrity and availability of IT services:

Housekeeping measures are required to maintain the integrity and availability of services.

Routine procedures will be established by computer staff for taking back-up copies of data, logging events and, where appropriate, monitoring the equipment environment.

Documented procedures for each system shall include:

- data back-up,
- operator logs,
- fault logging,
- environmental monitoring,
- network and application restart procedures,
- change request logs,
- system updates / upgrades.

6.6 Network Management

Objective:

To ensure the safeguarding of information in networks and the protection of the supporting infrastructure:

Appropriate controls must be implemented to ensure the security of data in networks and the protection of connected services from unauthorised access.

Each authorised user will be allocated a unique logon identifier by ICT Support staff and a password that the user must change at least every 90 days. The password must contain at least eight characters including a mixture of three of the following four elements (a complex password):

- lower case alpha characters,
- upper case alpha characters,
- numbers,
- special characters.

The password policy is to be reviewed on a yearly basis following guidance issued by NCSC.

Access to the network is automatically barred after four successive unsuccessful attempts to logon. Users are responsible for ensuring the secrecy and quality of their password and shall be held responsible for all actions recorded against their unique logon identifier.

The ICT Manager is responsible for ensuring the security of the networks.

A separate procedure document is available “Starters and Leavers Process Including Domain Account Administration” on the ICT intranet page.

6.7 Media Handling and Security

Objective:

To prevent damage to assets and interruptions to business activities:

Computer media containing data shall be controlled and physically protected.

Appropriate operating procedures will be established to protect computer media (tapes, disks, cassettes) input / output data and system documentation from damage, theft and unauthorised access.

At least one copy of all computer media containing data or critical software will be stored in media fire safes. A copy of all such media should also be kept securely offsite.

Computers that rarely physically connect to the network such as laptops or computers provided to members and some officers are not covered under our backup policy and data backups of these computers is the responsibility of the member or officer. A means of backing up the computer and a lesson on how to backup data will be provided by the ICT department

6.8 Data and Software Exchange

Objective:

To prevent loss, modification or misuse of data:

Exchanges of data or software between the Council and third parties should be managed in accordance with the data classification table in Appendix 1.

For critical or sensitive data and software, formal agreements, (including software escrow agreements where appropriate) for exchange of data and software (whether electronic or manual) between organisations should be established. These agreements should specify appropriate security conditions which reflect the sensitivity of the information involved, including:

- management responsibilities for controlling and notifying transmission, despatch and receipt,
- minimum technical standards for packaging and transmission,
- courier identification standards,
- responsibilities and liabilities in the event of loss of data,
- data and software ownership and responsibilities for data protection, software copyright compliance and similar considerations,
- technical standards for recording and reading data and software,
- any special measures required to protect very sensitive items
- The use of personal e-mails for sharing of data is prohibited

In order to ensure security of physical media in transit reliable transport couriers should always be used. Packaging should be sufficient to protect the contents from any physical damage during transit and should be in accordance with manufacturers' instructions.

Data in transit should be sealed with tamper proof or evidence devices and have accompanying documentation to list package contents.

All electronic commerce should be in accordance with the Council's Contract Procedure Rules / Financial Procedure Rules and subject to formal contract(s) drawn up between the Council and the trading partner(s), including the specialised areas of communication processes, transaction message security and data storage. Managers will need to obtain the appropriate specialised advice upon, identify and take into account all external and internal requirements affecting this activity. These requirements are likely to include the acts and directives listed in section 9.1 of this policy. Also relevant will be international and local (to other countries) laws and directives, any national or international professional regulations such as accounting practice and tax regimes, any conditions specified by the Council's insurers, fair trade and human rights standards, and the requisite information and technology standards

and controls to preserve the timeliness, accuracy and integrity, security, recoverability and processing of this activity.

6.9 Connection to Other Networks

Objective:

To facilitate use of this means of communication while preventing risks to the Council from inappropriate use:

For operational purposes, the Council will sometimes require access to external networks both to make use of business applications and to exchange data. Access to such networks is only allowed under the following conditions:

- must be authorised by the relevant Head of Service;
- must be agreed by the ICT manager or ICT Security Officer;
- must be protected by a firewall configured to provide protection of all networks concerned;
- must be subject to a suitable data sharing agreement / contract;
- must have protocols in place to protect data in transit and at rest.

6.10 Electronic Mail

Objective:

To facilitate use of this means of communication while preventing risks to the Council from inappropriate use:

Controls to reduce the security risks associated with electronic mail (e-mail) should be implemented covering:

- vulnerability to unauthorised interception or modification. Confidential data should only be sent in encrypted form;
- vulnerability to error, for example incorrect addressing;
- legal considerations such as the need for proof of origin, despatch, delivery and acceptance;
- publication of directory entries;
- remote access to e-mail accounts.

All staff have internal e-mail facilities, and external e-mail will be made available to all members and those officers with the authorisation of their director or head of service.

All use of e-mail shall be in accordance with the Electronic Communications Policy and Guidelines. Users shall avoid responding to unsolicited e-mails from unverifiable sources, and in particular, except where there is a justifiable business reason that has been expressly agreed with the ICT Manager, shall not open such mail or any attachments in such circumstances as there is a significant risk they may contain a virus. IT staff shall monitor usage of e-mail and report any concerns to the appropriate director or head of service.

All e-mail sent to external parties shall contain a standard disclaimer inserted by the e-mail system and in a form approved by the Council's Legal Officer.

All e-mail inbound and outbound will be subject to security scans for spyware, malware and viruses.

Electronic e-mail is not to be used via the Outlook App installed on personal devices.

Forwarding of e-mails to personal e-mail accounts is prohibited.

The use of personal e-mails for sharing of data is prohibited.

6.10.1 Confidential or RESTRICTED Information

Specific conditions apply to the use of RESTRICTED information:

- mail must not be forwarded to lower classification domains i.e. to organisations not within the government secure intranet network (GCSi) or government secure extranet (GCSx)

6.10.2 Use of E-mail Outside the UK

- **Due to the inherent increased security risk of accessing data via non-UK networks mail must not be accessed from outside the UK without the specific authorisation of the relevant Director.**
- Any user planning to do so must be aware of the relevant guidelines issued by FCO regarding the use of mobile telephones and IT services outside the UK.

6.11 Internet

Objective:

To facilitate use of this major source of information while preventing risks to the Council from inappropriate use:

The use of the Internet on the Council's computer systems shall be controlled and monitored to prevent:

- users wasting time and public resources by playing or "surfing" when they are paid to work;
- users accessing sites and importing material which the Council, as a matter of policy, may find unacceptable;
- users accessing sites and importing illegal material;
- users importing a virus or other malicious software and hence compromising the accuracy, availability and confidentiality of Council systems;
- users committing the Council to expenditure in an unauthorised fashion.

Internet access is to be used only for access to sites relevant to work or vocational training during an individual's working hours (this does not apply to members).

For staff in the main Council Offices this will be from 08:00 to 18:00 Monday to Friday. Officers using remote access facilities from home may use the Council's central internet connection between 07:00 and 22:30 on any day.

Personal use of the internet is permitted outside of staff's working hours and is subject to compliance with the Council's "Internet and E-mail Access - Conditions of Use" policy document.

This "Conditions of Use" policy will apply to those Members and Officers accessing the internet to view Web pages or to send / receive e-mails.

Internet access and e-mail is provided via a central connection to the internet which incorporates security features (intrusion detection and intrusion prevention) to safeguard the security and integrity of the Council's IT systems and data. This connection will always be used by Officers and members located at Council offices unless specifically authorised to use other methods. The key terms and conditions are as follows:

- Authority to use the Internet and/or e-mail facility will only be granted by the Chief Executive, Directors, Heads of Service or Service Managers.
- All Officers and Members using the facility will be required to sign the "Conditions of Use" document to confirm that they have read and agree to abide by its conditions. A breach of the conditions of use may result in disciplinary action and/or criminal proceedings.
- All "Conditions of Use" forms must be countersigned electronically or manually, by a designated authorising supervisor and completed documents will be held by the IT section and Human Resources section.
- All users of the facility will be issued with their own unique User ID and password and users will be deemed responsible for any activity logged against the user ID so User IDs and passwords should not be disclosed to other persons.
- The Council maintains logs of activity on our central Internet connection and may analyse and monitor those logs and all internet traffic.

Copies of the 'conditions of use' form are available on the Council's intranet or are available from the ICT department.

All access to the Internet will be traceable to an originating user ID, both currently and retrospectively.

All access and attempted access to the Internet will be logged by the IT section, and comprehensive information on usage, including the time and length of visits, will be supplied on request or in the event of concerns by the ICT Manager, to a user's director or head of service or Chief Executive in the case of members.

The IT section has implemented and maintains an automatic method for restricting which Internet sites may be accessed. No user shall attempt to access an Internet site which, from its address, may reasonably be considered to contain pornographic material or any other material prohibited by the "Conditions of use" policy. The corporate leadership team will define which sites are not to be accessed and any deliberate attempt to access such site/s will be considered in accordance with the disciplinary procedure.

Intrusion protection system (IPS) is in place, to detect, monitor, analyse and alert on attempted cyber-attacks.

Access to restricted and prohibited sites is automatically monitored and reports of activity will be made available to the user's director or head of service. A monthly security review will be conducted to ensure security and compliance, led by the ICT security officer.

The IT section has implemented and maintains a resilient security gateway device or “firewall” (software and hardware facilities) to control and vet and filter, incoming data to guard against recognised forms of Internet assaults and malicious software.

Only IT staff may download software, including freeware from the Internet. This does not apply to documents, i.e. Word, Excel, PDF format.

7. SYSTEM ACCESS CONTROL

7.1 Business Requirements for System Access

Objective:

To control access to business information:

Access to computer services and data should be controlled on the basis of business requirements, but accesses granted to a system should not compromise situations where separation (segregation) of duties is important.

Each system administrator will set up the system access rights of each user or group of users according to authorised business needs. Update access rights should be restricted to the minimum number of people commensurate with the need to maintain service levels.

System access controls are reviewed by Internal Audit during their routine systems audit work programme.

Domain privileged access will be reviewed periodically.

7.2 User Access Management

Objective:

To prevent unauthorised computer access:

Formal procedures will be developed for each system by the system administrator to cover the following:

- formal user registration and de-registration procedure for access to all multi-user IT services;
- restricted and controlled use of special privileges;
- Allocation of passwords securely controlled;
- ensuring the regular change and where appropriate quality and complexity of passwords;
- regular review of user access rights and privileged access rights;
- controlled availability of master passwords in emergencies.

A separate procedure document is available “Starters and Leavers Process Including Domain Account Administration” on the ICT intranet page.

User access will be suitably administered to ensure that the type of account granted to employees is such that it allows them to perform their day-to-day user activities and prevents access to any sensitive information not required for the purpose of undertaking their duties.

Ensuring members of staff, contractors and third party access to information systems does not exceed the needs of the role on a 'need to know' basis; that their use of ICT is appropriate and the starter, leaver and amendments changes are properly processed and authorised.

Network accounts which have not been logged into for 90 days will be reviewed and actioned taken. This activity will occur every 90 days to ensure accounts are disabled in quick and secure manner.

7.3 User Responsibilities

Objective:

To prevent unauthorised computer access:

Effective security requires the co-operation of authorised users. Users must comply with Council policies, standards and procedures regarding access controls, in particular the use of passwords and the security of equipment.

In order to maintain security users must:

- **not** write passwords down where others may readily discover them;
- **not** tell anyone else their password/s;
- **not** use obvious passwords such as their name;
- **not** let other people observe when entering their password;
- use a password with at least eight characters in it including numeric or special characters;
- promptly change their password if they suspect anyone else may be aware of it;
- log out of applications if they will be away from their desk for any length of time;
- 'lock' their PC when away from their desk to prevent it being used by others (by using Ctrl + Alt + Del keys or the Windows key + L key);
- if working at home the device must be shut down at the end of the day, so that security polices can be applied on next start up and stored in a secure location, when not in use;
- follow the Council's ICT security policy (including reading and signing confidentiality and conditions of use agreements);
- restart PCs and laptops as required after the application of security updates;
- report security incidents to the ICT Service Desk;
- not to open e-mails containing suspicious attachments;
- check e-mail and names of people they received a message from to ensure they are legitimate;
- report scams, privacy breaches and hacking attempts;
- do not re-use password from other systems.

Staff will be held responsible for all activities logged to their unique user ID.

7.4 Network Access Control

Objective:

Protection of networked services:

Connections to networked services shall be controlled in order to ensure that connected users or services do not compromise the security of any other networked services.

The ICT Manager is responsible for the protection of networked services.

All machines including servers are patched every month, this is the patch management cycle, to keep our estate up to date and protected.

A daily operations check is carried out as part of the daily checks procedure to ensure Antivirus, Antimalware and Anti Spyware updates are up to date on all PCs laptops and desktops

Devices not purchased by the ICT department are not to be plugged into or connected wirelessly to the Council's corporate network unless authorised by the ICT Manager or ICT Security officer.

All mobile devices and including tablets, laptops and smartphones will be encrypted using device management software.

7.5 Computer and Application Access Control

Objective:

To prevent unauthorised access to computers and information held:

Access to computer facilities should be restricted to authorised users. Computer facilities that serve multiple users should be capable of:

- identifying and verifying the identity of each authorised user, particularly where the user has update access;
- recording successful and unsuccessful attempts to access the system including files and folders;
- providing a password management system which ensures quality passwords;
- where appropriate restricting the connection times of users;
- controlling user access to data and system functions;
- restricting or preventing access to system utilities which override system or application controls;
- complete 'lock out' of user access after a pre-agreed number of unsuccessful attempts to access data.

8. SYSTEMS DEVELOPMENT AND MAINTENANCE

8.1 Security Requirements in Systems

Objective:

To ensure that security is built into IT systems and applications:

All security requirements, including a risk analysis and the need for fall back arrangements, should be identified at the requirements phase of a project by the officer requesting the system in consultation with computer and audit staff. Security requirements should be justified, agreed and documented.

The analysis of security requirements should:

- consider the need to safeguard the confidentiality, integrity and availability of information assets;
- identify controls to prevent, detect and recover from major failures or incidents;
- when specifying that a system requires a particular security feature, the quality of that feature must be specified, e.g. Password controlled - *“the password must be held in encrypted format. Passwords must expire after a number of days set by the system administrator, passwords should not be reusable, the system administrator should be able to specify a minimum length and other rules concerning password composition”*.

In order to ensure IT staff and users are aware of security controls in place, controls must be explicitly defined by the relevant system administrator in all relevant documentation.

8.2 Security of Application System Files

Objective:

To ensure that IT projects and support activities are conducted in a secure manner:

Access to application software, data files and system management files should be formalised and documented according to the sensitivity and importance of the system.

Maintaining the integrity of applications is the responsibility of the system administrator who will ensure that:

- strict control is exercised over the implementation of software on the operational system;
- test data is protected and controlled.

8.3 Security in Development and Support Environments

Objective:

To maintain the security of application systems software and data:

All proposed system changes must be reviewed to ensure they do not compromise the security of either the system or operating environment. The ICT Manager is responsible for all operating systems and the appropriate system administrator is responsible for the application. It is essential that both parties work together to ensure the security of application software and data is maintained.

Unsupported modifications to packaged software will only be authorised in exceptional circumstances. Wherever possible the required changes should be obtained from the vendor as standard program updates.

The implementation of any changes to systems should be strictly controlled using formal change control procedures. All system changes will be documented.

It should be a standard that any operational system has separate and secure test, training and development environments.

9. COMPLIANCE

9.1 Compliance with Legal Requirements and Codes of Practice

Objective:

The Council's statutory obligation to have sound information and cyber security arrangements in place originates in the Data Protection Act 1998, which states:

“Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and accidental damage or destruction of personal data.”

The Council depends on the confidentiality, integrity and availability of its information and ICT to such an extent however, that a serious breach of information security could impact on the Council's ability to deliver a wide range of statutory services.

In addition the Council has contractual obligations to ensure sound security if it is to use the Government Public Services Network (PSN) or receive or share information with partner agencies under information sharing arrangement

There are a number of laws which relate directly or indirectly to IT and its use and it is essential that these statutory requirements are met. Legislation which applies includes:

- The Copyright, Designs and Patents Act 1988
- The Data Protection Act 1998
- The Computer Misuse Act 1996
- Regulation of Investigatory Powers Act 2000
- The Human Rights Act 1998
- Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations 2000
- Health and Safety at Work etc Act 1974
- EC Directives.

In order to ensure security and integrity of data held and shared within both central government departments and local government the Council is obliged to adhere to set of standards defined in the 'code of connection' document issued by Department of Work and Pensions April 2008. The standard must be met before government departments such as Department of Work and Pensions will share data with the Council

Note: Failure to adhere to the required standard will result in electronic data sharing with government departments being suspended.

9.1.1 Control of Proprietary Software Copying

Objective:

To ensure that the Council complies with current legislation:

Proprietary software is usually supplied under a licence agreement which limits the number of users and/or limits the use to a specified machine. Copyright infringement can lead to legal action, fines and adverse publicity.

It is Council policy that no copyright material is copied without the owner's consent.

9.1.2 Use of Unlicensed Software

Except for freeware, the use of unlicensed software amounts to theft and the Council's policy is only to use licensed software. The Federation Against Software Theft (FAST) and the Business Software Alliance are particularly active in detecting and prosecuting organisations (especially councils) who use unlicensed software.

The introduction and/or use of unlicensed software is prohibited and may be treated as gross misconduct.

9.1.3 Safeguarding of the Council's Records

Important records must be protected from loss, destruction and falsification. All financial records need to be retained for seven years or more to meet audit requirements.

All historic data should be periodically archived by the relevant system administrator with copies being retained in media fire safes on and off site, in accordance with GDPR regulations.

9.1.4 Auditing and logging the use of ICT resources

The Council maintains audit logs of events taking place across its complete network. This includes, but not limited to:

- user login times;
- details of failed login attempts;
- details of access to data files and software applications (user ID, times);
- details of any privileged access to system;
- software and hardware configuration changes;
- details of internet web usage and restricted access reports;
- details of files, folder and network access to objects.

9.1.5 Data Protection

Personal information on living individuals who can be identified from the information that is stored or processed on a computer is subject to data protection legislation. The Data Protection Act 2018 extended this to information held in certain paper based systems. Disclosure of information is also governed by the Freedom of Information Act 2000.

The officer responsible within the Council for data protection is the Records Management Officer who will provide guidance to managers and other staff on their individual responsibilities and the specific procedures that should be followed.

It is a manager's responsibility to inform either the ICT Manager or the Records Management Officer of any proposals to keep personal information on a computer and any changes in the use for which data is kept. With the assistance of the Records Management Officer, managers must ensure that the relevant staff are made aware of the data protection principles defined in the legislation.

The Council is required to register details of the data kept, the purposes to which it is applied and to whom it may be disclosed. It is a manager's responsibility to ensure that the registration is accurate and amended when necessary and to take note of any advice from the Information Commissioner before undertaking any data matching exercise.

Under the Act staff could be held legally responsible for the confidentiality of personal data. Staff must be very careful as to whom they disclose information to and be aware of the need for security of information in any format including printed documents and electronic mail. **Particular care must be taken in disclosing personal data on the telephone, if in any doubt as to the identity of a caller personal data must not be disclosed on the telephone.**

The six principles of the Data Protection Act are that personal data should be:

- processed lawfully, fairly, and in a transparent manner relating to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
- processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

9.1.6 Prevention of Misuse of IT Facilities

The Council's computer facilities are provided for Council business or in connection with approved study courses. Staff and members are allowed to use the Council's computer facilities for personal use for the following:

- personal use of e-mail in accordance with the "Internet and E-Mail Access – Conditions of Use" policy document;
- access to the Internet, if granted for work purposes, in accordance with the Internet and E-Mail Access - Conditions of Use" policy document;
- limited use of PC software, particularly word processing, in their own time.

The following conditions will apply:

- all private printing must be paid for unless an agreement has been reached with the ICT Manager or the printing service;
- unauthorised or excessive personal use may be subject to disciplinary action;
- The Computer Misuse Act 1990 introduced three criminal offences:
 1. unauthorised access;
 2. unauthorised access with intent to commit a further serious offence;
 3. unauthorised modification of computer material, i.e. alteration, erasure or addition to programs or data.

Users should not attempt to gain access to systems they are not authorised to use or see, as they could face criminal prosecution.

9.2 Security Reviews of IT Systems

Objective:

To ensure compliance of systems with the Council's ICT and Cyber Security Policy and standards:

The internal and external security of IT systems including external penetration testing, will be regularly reviewed and subject to cyber security and penetration testing

This will be carried out by an approved CREST/IASME

The review of security processes will be carried out by Internal Audit, External Audit and managers

ICT will use specialist third parties to perform external and internal security and cyber security health checks, annually in order to maintain the Cyber Essential PLUS accreditation as well as meeting out PSN security obligations.

Annual reviews will ensure compliance and assurance with the security policy, standards and best practice.

9.3 System Audit Considerations

Objective:

To minimise interference to / from the system audit process:

Audit requirements and activities involving checks on operational systems shall be carefully planned and agreed to minimise the risk of disruptions to business processes.

There should be controls to safeguard operational systems and audit tools during system audits.

The following are to be observed:

- audit requirements to be agreed with the appropriate manager;
- the scope of any checks to be agreed and controlled;
- checks to be limited to read only access to software and data wherever possible;
- access, other than read only, only to be allowed for isolated copies of system files which must be erased when the audit is completed;
- IT resources for performing checks should be identified and made available;
- requirements for special or additional processing should be identified and agreed with service providers;
- wherever possible access should be logged and monitored;
- all procedures and requirements should be documented.

Access to system audit tools should be controlled.

THE NATIONAL PROTECTIVE MARKING SCHEME FRAMEWORK

The National Protective Marking System provides a framework for users to share and protect information in an appropriate manner. As can be seen from the table, each protective marking is allocated an appropriate Impact Level (IL). Each IL describes a severity of impact to the UK of protectively marked information being released outside of normal government handling channels.

The IL value is used by security officers when performing a risk assessment on protectively marked information in order to determine how much protection these assets should be given.

Protective Marking	Impact Level
TOP SECRET	6
SECRET	5
CONFIDENTIAL	4
RESTRICTED	3
PROTECT	2 1
Unclassified	0

On 28 February 2007 the new sub-national caveat, PROTECT, was introduced. The purpose of PROTECT is to provide a difference in terms of the handling official information which needs to be protected from compromise of confidentiality, integrity and availability to a known level of assurance, but for which the measures required to safeguard National Security information at RESTRICTED are considered not to always meet the direct business need of the organisation. It is envisaged that in some organisations the use of RESTRICTED will be reduced as a consequence.

At the Local Authority level and for users of GCSx it is envisaged that most protectively marked information will be of 'PROTECT' in nature.

At a working level the baseline security objectives for PROTECT will be the same as for RESTRICTED, which are:

- handle, use and transmit with care;
- take basic precautions against accidental compromise or opportunist attack.

The distinction between the two markings is that PROTECT is not a National Security marking, and there is a revised calculation for asset value, or consequence of compromise. Depending on the severity of the circumstances either RESTRICTED or PROTECT may apply where compromise would be likely to:

- cause financial loss or loss of earning potential to, or facilitate improper gain or advantage for, individuals or companies;

- prejudice the investigation or facilitate the commission of crime;
- disadvantage government in commercial or policy negotiations with others.

N.B. Within the UK Government, CONFIDENTIAL is an explicit marking with clearly defined handling requirements. Sometimes, within certain local authorities 'Confidential' is used as a marking to indicate that information has a requirement for protection (in UK Government terms it is protectively marked). Care should be taken to ensure that information protectively marked with the national CONFIDENTIAL marking should be handled accordingly.

The PROTECT Classification

Guidelines	<ul style="list-style-type: none"> • Cause substantial distress to individuals. • Breach proper undertakings to maintain the confidence of information provided by third parties. • Breach statutory restrictions on the disclosure of information.
Principles and Clearance Levels	<ul style="list-style-type: none"> • Information classified as PROTECT should be held, processed, transmitted and destroyed with discretion to make compromise highly unlikely. • Only staff cleared by the organisation to access PROTECT level or above are authorised to handle the information. This includes all staff involved with transmission, storage and disposal.
Electronic Transmission	PROTECT information transmitted across public networks within the UK or across any networks overseas should be encrypted using an approved system.
Electronic Storage	<p>Electronic files (including databases) must be protected against illicit internal use or intrusion by external parties through a judicious selection of two or more of the following mechanisms:</p> <ol style="list-style-type: none"> a. User challenge and authentication (username / password or digital ID / Certificate). b. Logging use at level of individual. c. Firewalls and intrusion-detection systems and procedures; server authentication. d. OS-specific / application-specific security measures.
Electronic Disposal	Electronic files should be disposed of in a way that makes reconstruction highly unlikely.
Voice Telephone Conversation	Information protectively marked with PROTECT can be spoken about over the telephone.
Manual Transmission	<ul style="list-style-type: none"> • Within a single physical location. As determined by the information security officer. • Transfer between establishments within or outside UK: <ol style="list-style-type: none"> a. May be carried by ordinary postal service or commercial courier firms, provided the envelope / package is closed and the word PROTECT is not visible. b. The outer envelope should be addressed to an individual by name and title. PROTECT mail for / from overseas posts should be carried by diplomatic airfreight.

	c. The outer envelope must clearly show a return address in case delivery is unsuccessful. In some cases due to the nature of the contents, identifying the originating organisation may be inappropriate and a return PO Box alone should be used.
Manual Storage	<ul style="list-style-type: none"> • In an office environment, PROTECT material should be held in a lockable storage area or cabinet. • In a storage facility, all material should be protected through controlled access to the storage areas, and through a secure physical environment.
Manual Disposal	Disposed of or destroyed in a way that makes reconstruction highly unlikely.

The RESTRICTED Classification

Guidelines	<ul style="list-style-type: none"> • Affect diplomatic relations adversely. • Hinder the operational effectiveness or security of the UK or friendly forces. • Affect the internal stability or economic well-being of the UK or friendly countries adversely.
Principles and Clearance Levels	<ul style="list-style-type: none"> • Information classified as RESTRICTED should be held, processed, transmitted and destroyed with discretion to make compromise highly unlikely. • Only staff cleared by the organisation to access RESTRICTED level or above is authorised to handle the information. This includes all staff involved with transmission, storage and disposal.
Electronic Transmission	All RESTRICTED information transmitted across public networks within the UK or across any networks overseas must be encrypted using an approved system.
Electronic Storage	Electronic files (including databases) must be protected against illicit internal use or intrusion by external parties through a judicious selection of two or more of the following mechanisms: <ul style="list-style-type: none"> a. User challenge and authentication (username / password or digital ID / Certificate). b. Logging use at level of individual. c. Firewalls and intrusion-detection systems and procedures, server authentication. d. OS-specific / application-specific security measures.
Electronic Disposal	Electronic files should be disposed of in a way that makes reconstruction highly unlikely.
Voice Telephone Conversation	Telecommunications made at RESTRICTED (Confidentially IL 3) level can no longer be guaranteed as secure. Appropriate secure communications should be used.
Manual Transmission	<ul style="list-style-type: none"> • Within a single physical location. As determined by the information security officer.

	<ul style="list-style-type: none"> • Transfer between establishments within or outside UK: <ul style="list-style-type: none"> a. May be carried by ordinary postal service or commercial courier firms, provided the envelope / package is closed and the word RESTRICTED is not visible. b. The outer envelope should be addressed to an individual by name and title c. The outer envelope must show clearly a return address in case delivery is unsuccessful. In some cases, due to the nature of the contents, identifying the originating organisation may be inappropriate and a PO box should be used.
Manual Storage	<ul style="list-style-type: none"> • In an office environment, RESTRICTED material should be held in a lockable storage area or cabinet. • In a storage facility, all material should be protected through controlled access to the storage areas, and through a secure physical environment.
Manual Disposal	Disposed of or destroyed in a way that makes reconstruction highly unlikely.

Major Differences Between PROTECT and RESTRICTED

For Local authorities such as NWLDC the two protective markings which will be most commonly seen in the workplace are PROTECT and RESTRICTED. Out of these two protective markings it is anticipated that PROTECT will be the most common.

Information with the PROTECT protective marking will be handled in the same way as RESTRICTED in most circumstances. The primary difference is that Council Staff will be allowed to have telephone conversations with regard to information protectively marked as PROTECT. Information protectively marked as RESTRICTED is not allowed to be passed over the telephone.

INTERNET & EMAIL ACCESS – CONDITIONS OF USE

A) Introduction

The purpose of the following Conditions of Use is to safeguard the security and integrity of the Council's Information Technology systems. It outlines your personal responsibilities and informs what you must & must not do.

These conditions of use apply to, but are not limited to, all North West Leicestershire District Council Councillors, Committees, Departments, Partners, Employees of the Council, contractual third parties and agents of the Council who access the Councils Internet service and IT equipment.

These conditions should be applied at all times whenever using the Council provided Internet & e-mail facility. This includes access via any access device including desktop computers, laptops, notebooks or Smartphone devices.

Authority to access the Internet and e-mail facilities may only be granted by Corporate Leadership Team, Heads of Service or Service Managers. All members and staff authorised to access these facilities will be required to confirm, in writing, that they have read and agree to abide by these Conditions of Use which may be amended from time to time.

Users should be aware that usage of the Internet and e-mail may be monitored to ensure compliance with these conditions or where there may be a breach of these conditions. Further details on such monitoring are attached at Appendix 1, which forms part of the Conditions of Use.

The Internet facility is made available for the business purposes of the Council. A certain level of personal use is permitted in accordance with conditions defined within this document.

In these conditions, 'Internet' means the World Wide Web and 'e-mail' means the use of the Council's internal electronic mail system or the external Internet electronic mail system.

B) Conditions of Use

1. General

- 1a. Users may only access Internet & email services using hardware and software installed for that purpose. Users must not interfere with the configuration of the software.
- 1b. The Council provides a secure login ID and password for all users of Council ICT facilities and this login ID & password is also used to access the internet and e-mail.

The Council's ICT department is responsible for the technical management of these logins

- 1c. Users must treat the information gleaned from the Internet with caution giving due consideration to its unregulated nature. For the purpose of these Conditions of Use, the term 'information' is deemed to include text, data, images or any other material.
- 1d. Users must not disclose their User-ID's and / or passwords to other persons. All access to internet or e-mail services must be completed using the users own unique User-ID and password. Users will be deemed responsible for all activity logged to their User-ID.
- 1e. Users must report any known or perceived breach of security to the ICT Service Desk immediately.
- 1f. A breach of these Conditions of Use may result in disciplinary action and/or criminal proceedings.

2. Internet

- 2a. Private use of the Internet is permitted but Officers using these facilities for their private purposes must do so outside of their working hours and must adhere to the conditions stated at 2b to 2i at all times. Except for this provision for private use, use of the Internet shall be restricted, specifically during core times, to the proper conduct of the Council's business only. Use of the Internet shall at all times be carried out in a manner which does not prejudice the Council as a responsible provider of public services.
- 2b. The Internet must not be used to upload (*send*) information in plain text form which might be regarded as sensitive or confidential. This includes both personal and commercially sensitive information which should continue to be sent by conventional means.
- 2c. Council equipment must not be used for the storage of files or any other information not related to Council business.
- 2d. the use of Internet Instant Messenger and chat rooms is not permitted.
- 2e. Users are expressly forbidden from downloading (*receiving*) or viewing from the Internet information, data, images or any other material which is of a pornographic, racist, sexist, homophobic or other discriminatory nature, or extreme political nature, or which incites violence, hatred, illegal activity or abuse in any form. Where possible, such sites have been blocked, however, any user who accidentally accesses such information, data, images or material must immediately notify the ICT Manager or the ICT Service desk. This is to protect you from Condition 1f above.
- 2g. No software is to be downloaded from the Internet without the prior written consent of either the ICT Manager or the ICT Infrastructure & Security Manager and prior to such downloading, Users must refer to the Council's ICT Security Policy. If the software is to be used on a continuing basis and is subject to any licensing arrangement (e.g. registration of shareware with the publisher), it must be properly registered in accordance with the publisher's requirements and recorded in the Council ICT asset database.

- 2h. In general terms, any use of the Internet which contravenes any legal Act (for example, The Data Protection Act 1998, The Computer Misuse Act 1990, The Copyrights, Designs and Patents Act 1988), or any internal Council policy is unacceptable.
- 2i. A council computer cannot be used for private purposes if, at that time, it is required for use on Council business.
3. E-mail
- 3a. Use of the Councils e-mail facilities (both internal and external) shall be restricted primarily to the proper conduct of the Council's business only and shall at all times be carried out in a manner which does not prejudice the Council as a responsible provider of public services. The Council recognises that e-mail forms a modern form of communication. To this end, the e-mail facility may be used for occasional [essential] private communications. No charge will be made at present. Frequent or excessively long e-mails may require explanation. Personal e-mail messages must not be retained for longer than absolutely necessary within the Councils e-mail system.
- 3b. the e-mail facility must not be used to upload (*send*) information in any form which might be regarded as sensitive or confidential. This includes both personal and commercially sensitive information which should continue to be sent by conventional means.
- 3c. Any user who receives, information, data, images or any other material which is of a pornographic, racist, sexist, homophobic or other discriminatory nature, or extreme political nature, or which incites violence, hatred, illegal activity or abuse in any form such information, data, images or material must immediately notify the ICT Manager or the ICT Service Desk. This is to protect you from Condition 1f above. The item should then be deleted and not forwarded to other people.
- 3d. Users must not disclose their user-ID and / or passwords to other persons. Users will be deemed responsible for all activity logged to their User-ID. The Council reserves the right to and does monitor both incoming and outgoing e-mails.
- 3e. the exchange of all electronic mail both internal and external shall at all times be professional and courteous. Official correspondence using the Internet electronic mail must be subject to such management review as is currently in place for posted correspondence.
- 3f. Where a User has been assigned an e-mail address relating to the Division or Section, it is the Users responsibility to ensure that she/he does not disclose any passwords associated with that e-mail address.

C) Internet and e-mail monitoring.

E-mail

The Council reserves the right to monitor employees' e-mails, but will endeavor to inform an affected employee when this is to happen and the reasons for it. The Council considers the following to be valid reasons for checking an employee's e-mail:

If the employee is absent for any reason and communications must be checked for the smooth running of the Council to continue.

If the Council suspects that the employee has been viewing or sending material, of a pornographic, racist, sexist, homophobic or other discriminatory nature, or of an extreme political nature. or material which incites violence, hatred illegal activity or abuse in any form.

The Council understands that it is possible for employees inadvertently to view such material and they will have the opportunity to explain if this is the case).

If the Council suspects that an employee has been using the e-mail system to send and receive an excessive number of personal communications.

If the Council suspects that the employee is sending or receiving e-mails that are detrimental to the Council.

When monitoring e-mails, the Council will, save in exceptional circumstances, confine itself to looking at the address and heading of the e-mails. Employees should mark any personal e-mails as such and encourage those who send them to do the same. The Council will avoid, where possible, opening e-mails clearly marked as private or personal.

The Council reserves the right to retain information that it has gathered on employees' use of e-mail for a period of one year.

Internet

All use of the Council's internet service is logged and recorded for the purposes of:

- Monitoring total usage to ensure the business use is not affected by lack of capacity.
- Filtering content to prevent access to unsuitable material
- Producing reports and statistics for senior managers

The Council reserves the right to monitor specific employees' internet usage but will endeavor to inform an affected employee when this is to happen and the reasons for it. The Council considers the following to be valid reasons for checking an employee's internet usage: -

- If the Council suspects that the employee has been viewing material, of a pornographic, racist, sexist, homophobic or other discriminatory nature, or of an extreme political nature or material which incites violence, hatred illegal activity or abuse in any form.

- The Council understands that it is possible for employees inadvertently to view such material and they will have the opportunity to explain if this is the case.

- If the Council suspects that the employee has been spending an excessive amount of time viewing websites that are not work related.

The Council reserves the right to retain information that it has gathered on employees' use of the internet for a period of one year.

When used for private purposes, the Computer, any data held on it or any other activity logs remain the property of the Council and may be accessed at any time by the Council to ensure compliance with all of its statutory, regulatory & internal policy requirements.

SIGN BELOW TO ACCEPT THE ICT SECURITY POLICY AND HAND THE FORM TO THE ICT DEPARTMENT

**North West Leicestershire District Council
Information and Communications Technology (ICT) and Cyber
Security Policy**

North West Leicestershire District Council is dependent upon its Information and Communications Technology (ICT) systems for its normal day to day business activities. It is therefore essential for the continued successful operation of the Council that the confidentiality, integrity and availability of its ICT systems and data are maintained at a high level. There is also an obligation on the Council and all employees, contractors and advisors to comply with the relevant legislation such as the Data Protection Acts, the Copyright, Designs and Patents Act and the Misuse of Computers Act.

It follows that a high standard of information security is required within the Council. To achieve this, the ICT and Cyber Security Policy has been adopted and everyone who uses IT equipment or accesses Council information must read the policy and ensure that they understand the obligations contained within it.

Once you have **read** and **understood** the ICT and Cyber Security Policy please sign and return the slip below to the ICT Service Desk.

North West Leicestershire District Council ICT and Cyber Security and Policy can be found on our intranet site

✂-----✂

**North West Leicestershire District Council
Information and Communications Technology (ICT) and Cyber
Security Policy**

I have read and understand the North West Leicestershire District Council's ICT Security Policy.

Print Name _____ Signed _____ Date _____

(Note: When completed, this should be forwarded to the IT Section, who will copy it to the Human Resources Section)

**NORTH WEST LEICESTERSHIRE DISTRICT COUNCIL -
GCSx PERSONAL COMMITMENT STATEMENT**

I understand and agree to comply with the security rules of my organisation as well as the GCSx Code of Connection.

For the avoidance of doubt, the security rules relating to secure e-mail and IT systems usage include:

1. I acknowledge that my use of the GCSx may be monitored and/or recorded for lawful purposes.
2. I agree to be responsible for any use by me of the GCSx using my unique user credentials (user ID and password, access token or other mechanism as provided) and e-mail address.
3. I will not use a colleague's credentials to access the GCSx and will equally ensure that my credentials are not shared and are protected against misuse.
4. I will protect such credentials at least to the same level of secrecy as the information they may be used to access, (in particular, I will not write down or share my password other than for the purposes of placing a secured copy in a secure location at my employer's premises).
5. I will not attempt to access any computer system that I have not been given explicit permission to access.
6. I will not attempt to access the GCSx other than from IT systems and locations which I have been explicitly authorised to use for this purpose.
7. I will not transmit information via the GCSx that I know, suspect or have been advised is of a higher level of sensitivity than my GCSx domain is designed to carry.
8. I will not transmit information via the GCSx that I know or suspect to be unacceptable within the context and purpose for which it is being communicated.
9. I will not make false claims or denials relating to my use of the GCSx (e.g. falsely denying that an e-mail had been sent or received).
10. I will protect any sensitive or not protectively marked material sent, received, stored or processed by me via the GCSx to the same level as I would paper copies of similar material.
11. I will not send Protectively Marked information over public networks such as the Internet.
12. I will always check that the recipients of e-mail messages are correct so that potentially sensitive or protectively marked information is not accidentally released into the public domain.
13. I will not auto-forward e-mail from my GCSx account to any other non-GCSx e-mail account.

14. I will disclose information received via the GCSx only on a 'need to know' basis.
15. I will not forward or disclose any sensitive or protectively marked material received via the GCSx unless the recipient(s) can be trusted to handle the material securely according to its sensitivity and forwarding is via a suitably secure communication channel.
16. I will seek to prevent inadvertent disclosure of sensitive or protectively marked information by avoiding being overlooked when working, by taking care when printing information received via the GCSx (e.g. by using printers in secure locations or collecting printouts immediately they are printed, checking that there is no interleaving of printouts, etc) and by carefully checking the distribution list for any material to be transmitted.
17. I will securely store or destroy any printed material.
18. I will not leave my computer unattended in such a state as to risk unauthorised disclosure of information sent or received via the GCSx (this might be by closing the e-mail program, logging-off from the computer, activate a password-protected screensaver, etc, so as to require a user logon for activation).
19. Where my organisation has implemented other measures to protect unauthorised viewing of information displayed on IT systems (such as an inactivity timeout that causes the screen to be blanked or to display a screensaver or similar, requiring a user logon for reactivation), then I will not attempt to disable such protection.
20. I will make myself familiar with the security policies, procedures and any special instructions that relate to the GCSx.
21. I will inform my manager immediately if I detect, suspect or witness an incident that may be a breach of security.
22. I will not attempt to bypass or subvert system security controls or to use them for any purpose other than that intended.
23. I will not remove equipment or information from my employer's premises without appropriate approval.
24. I will take precautions to protect all computer media and portable computers when carrying them outside my organisation's premises (e.g. leaving a laptop unattended or on display in a car such that it would encourage an opportunist thief).
25. I will not introduce viruses, Trojan horses or other malware into the system or GCSx.
26. I will comply with the Data Protection Act 1998 and any other legal, statutory or contractual obligations that my employer informs me are relevant.
27. If I am about to leave my employer, I will inform my manager prior to departure of any important information held in my account.
28. The GCSx Acceptable Usage Policy specifically states that all PROTECT and RESTRICT information will be appropriately labelled when sent over the GCSx and that public networks will not be used to send RESTRICT or PROTECT information.

29. I understand that use of GCSx / PSN services is subjected to Criminal conviction checks and I will declare any unspent convictions including cautions, reprimands, warnings, investigations or pending prosecutions to Human Resources.

**PLEASE SIGN BELOW TO ACCEPT THE GCSx SECURITY POLICY
AND HAND THE FORM TO THE ICT DEPARTMENT**

Name: Dept:

Signed: Date:

Authorised: Date:

This form can only be authorised by Team Managers or members of
CLT.

(Note: When completed, this should be forwarded to the IT Section, who will copy it to the Human Resources Section)

THIRD PART NETWORK ACCESS AGREEMENT

1. Purpose

The purpose of this agreement is to outline the specific terms and conditions governing the access and use of the North West Leicestershire District Council (NWLDC) network and information technology resources by the Third Party.

This agreement is dated and made between **North West Leicestershire District Council** and the following Third Party:

Company name:	[]
Address:	[]
	[]
	[]
Contact Name:	[]
Phone number:	[]
E-mail address:	[]

2. Definitions

Third parties are defined as any individual, consultant, contractor, vendor or agent not registered as a NWLDC employee.

Third party access is defined as all local or remote access to the NWLDC network for any purpose.

NWLDC network includes all data, applications, systems, services, infrastructure and computer devices which are owned or leased by the NWLDC.

Mobile computer devices are defined as any handheld computer device, including but not limited to laptops, notebooks, tablet computers, smartphone devices (e.g. PDA, iPhone and Blackberry enabled devices, etc).

Removable storage devices are defined as any optical or magnetic storage device or media, including but not limited to floppy disks, CD, DVD, magnetic tapes, ZIP disk, USB flash drive (i.e. memory stick / pen / keys), external / portable hard drives and SD Cards.

3. Terms and Conditions

In consideration of NWLDC engaging the Third Party for services requiring third party access and allowing such third party access, the Third Party agrees to the following:

- (a) The Third Party may only use the network connection for approved business purposes as specified by NWLDC and in accordance with NWLDC ICT policies. The use of the network connection for unapproved purposes, including but not limited to personal use or gain is strictly prohibited.
- (b) The Third Party may only use access methods which have been defined by the NWLDC ICT Services.

- (c) The Third Party must ensure that only their employees that have been nominated by the Third Party and approved by the NWLDC in advance, have access to the network connection or any NWLDC owned equipment.
- (d) The Third Party shall be solely responsible for ensuring its nominated employees are not security risks, and upon request from the NWLDC, the Third Party will provide the NWLDC with any information reasonably necessary for the NWLDC to evaluate security issues.
- (e) The Third Party will promptly inform the NWLDC in writing of any relevant employee changes. This includes the rotation and resignation of employees so that NWLDC can disable their usernames and remove / change passwords in order to secure its resources.
- (f) As part of any service agreement review the Third Party will provide the NWLDC with an up to date list of their employees who have access to the network connection or any NWLDC owned equipment.
- (g) The Third Party is solely responsible for ensuring that all usernames and passwords issued to them by the NWLDC remain confidential and are not used by unauthorised individuals. The Third Party must immediately contact NWLDC if they suspect these details have been compromised.
- (h) The Third Party will be held responsible for all activities performed on the NWLDC network while logged in under their usernames and passwords.
- (i) The Third Party must ensure at all times that all computer devices used by them to connect to the NWLDC network have reputable up to date anti-virus software and the appropriate security patches installed.
- (j) Only in exceptional circumstances and with the prior written approval of the NWLDC should the Third Party hold NWLDC information on mobile computer devices or removable storage devices. Should the business requirements necessitate the Third Party to store NWLDC information on mobile computer devices or removable storage devices, the Third Party must ensure that only the absolute minimum amount of information as is absolutely necessary is stored on the mobile computer device or removable storage device and the information is securely deleted when it is no longer required. The Third Party must ensure that all NWLDC information stored on mobile computer devices and removable storage devices belonging to the Third Party is encrypted to standards approved by NWLDC. Under no circumstance encrypted or otherwise should NWLDC information be stored by the Third Party on USB memory keys / sticks.
- (k) The Third Party must ensure that all mobile computer devices used by them to connect to the NWLDC network, are used in such a way that information belonging to the NWLDC is not displayed to unauthorised individuals or the general public.
- (l) The Third Party must ensure that all their computer devices connected to the NWLDC network are not connected to any other network at the same time, with the exception of networks that are under the complete control of the Third Party.
- (m) When the Third Party is connected to the NWLDC network they should not leave their computer devices unattended.

- (n) The Third Party must ensure that when they are connected to NWLDC network their activity does not disrupt or interfere with other non-related network activity.
- (o) All Third Party computer devices used to connect to the NWLDC network must, upon request by NWLDC be made available for inspection.
- (p) The Third Party network connection will by default be granted read / execute privileges only. All requests for increased privileges must be submitted in writing to the NWLDC where they will be considered on a case by case basis.
- (q) For security reasons all Third Party remote access accounts except those providing 24*7 support may be switched off (de-activated) by default. The Third Party will be required to e-mail (can be followed by phone) NWLDC ICT Services requesting that their account be switched-on (activated) for a stipulated period.
- (r) The Third Party must obtain the written consent of the NWLDC before implementing any updates or amendments to the NWLDC network, information systems, applications or equipment. All approved updates and amendments implemented by the Third Party must be made in line with NWLDC policies and procedures.
- (s) The Third Party must ensure all software is scanned and cleared of all viruses and other forms of malicious software before it is installed on any NWLDC information systems, applications or equipment. The Third Party will be held responsible for all disruptions and damage caused to the NWLDC network, information systems, applications or equipment which is traced back to infected software installed by the Third Party.
- (t) The Third Party and their employees must comply with all UK, European and NWLDC rules and regulations concerning safety, environmental and security operations while on-site at an NWLDC site. All Third Party personnel must carry photographic identification with them when they are on-site at an NWLDC facility.
- (u) Where the Third Party has direct or indirect access to NWLDC information, this information must not be copied, divulged or distributed to any other party without the prior written approval of the NWLDC.
- (v) The Third Party must report all actual and suspected security incidents to the NWLDC immediately.
- (w) The Third Party must manage and process all NWLDC information which they acquire from the NWLDC in accordance the Data Protection Act 1998 (as amended or replace) and any associated guidance.
- (x) The NWLDC reserves the right to:
 - Monitor all Third Party activity while connected (local and remote) to the NWLDC network.
 - Audit contractual responsibilities or have those audits carried out by an NWLDC approved third party
 - Revoke the Third Party's access privileges at any time.
- (y) On completion of the services requiring third party access, the Third Party must return all equipment, software, documentation and information belonging to the NWLDC.

- (z) Any violations of this agreement by the Third Party, may lead to the withdrawal of NWLDC network and information technology resources to that Third Party and/or the cancellation of any contract(s) between the NWLDC and the Third Party.

The Third Party agrees to abide by the terms and conditions of this agreement at all times.

Signed (On behalf of the Third Party):

Authorised Signature:

Name (Printed):

Title or Position:

Date:

This page is intentionally left blank

LOCAL CODE OF CORPORATE GOVERNANCE

Version No.	Author	Date	Summary of Changes
1		2009	
2	Tracy Bingham	October 2017	
3	Tracy Bingham	May 2020	
4	Dan Bates	June 2021	
5	Mark Walker	May 2022	
6	Glenn Hammons	July 2023	New section on the current challenges facing the Council

Version 6

July 2023

	Contents	Page No.
1.	Introduction	3
2.	Summary of Commitment	5
3.	Fundamental Principles of Corporate Governance	5

NORTH WEST LEICESTERSHIRE DISTRICT COUNCIL

Local Code of Corporate Governance

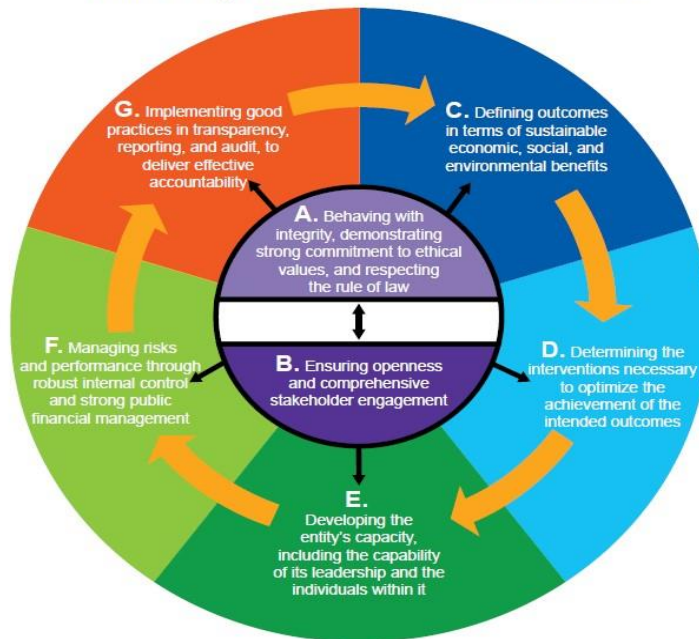
1 INTRODUCTION

- 1.1 In 2014, the Chartered Institute of Public Finance and Accountancy (CIPFA) and the International Federation of Accountants (IFAC) collaborated to produce The International Framework: Good Governance in the Public Sector. The International Framework defines governance as comprising the arrangements put in place to ensure that intended outcomes for stakeholders are defined and achieved. It states that in order to deliver good governance in the public sector, both governing bodies and individuals working for public sector entities must try to achieve their entity's objectives while acting in the public interest at all times.
- 1.2 The Chartered Institute of Public Finance and Accountancy in association with SOLACE have published their Framework entitled 'Delivering Good Governance in Local Government 2016'.
- 1.3 The diagram below¹ illustrates the core principles of good governance in the public sector and how they relate to each other: Principles A and B permeates implementation of principles C to G.

Achieving the Intended Outcomes While Acting in the Public Interest at all Times

¹ CIPFA/SOLACE Delivering Good Governance in Local Government Framework 2016

**Achieving the Intended Outcomes
While Acting in the Public Interest at all Times**



- 1.4 In North West Leicestershire, good governance is about how the Council ensures that it is doing the right things, in the right way and for the benefit of the communities it serves. The starting place for good governance is having shared values and culture and a framework of overarching strategic policies and objectives underpinned by robust systems and processes for delivering these.
- 1.5 By ensuring good governance is in place, the Council will ensure it has high standards of management, strong performance, the effective use of resources and good outcomes which in turn will lead to increased public trust.
- 1.6 The Council is committed to the seven core principles of good practice contained in the CIPFA framework and will test its governance arrangements against this framework and report annually (via its annual assurance review and Annual Governance Statement).
- 1.7 These seven core principles, also known as the Nolan Principles - The Seven Principles of Public Life, apply to anyone who works as a public office-holder. This includes all those who are elected or appointed to public office, nationally and locally, and all people appointed to work in the Civil Service, local government, the police, courts and probation services, non-departmental public bodies (NDPBs), and in the health, education, social and care services. A link to the Government website setting out the principles is below:

<https://www.gov.uk/government/publications/the-7-principles-of-public-life/the7-principles-of-public-life--2>

2 SUMMARY OF COMMITMENT

2.1 By adopting this Local Code of Corporate Governance, we are responding to the CIPFA/SOLACE Joint Working Group Guidance and Framework entitled 'Delivering Good Governance in Local Government'.

2.2 In doing so we will:

- Accept the core principles set out in section 3 below as the basis for our Corporate Governance arrangements.
- Publish an Annual Governance Assurance Statement with the Council's Statement of Accounts.
- Draw up Action Plans of improvements to our corporate governance arrangements, such plans to be monitored by the Audit and Governance Committee.

3 FUNDAMENTAL PRINCIPLES OF CORPORATE GOVERNANCE

3.1 Set out in this document is the Council's proposed Local Code of Corporate Governance which is based on the seven core principles (as set out in the illustration above) adopted for local government from the report of the Independent Commission on Good Governance in Public Services.

Principle A - Behaving with integrity, demonstrating strong commitment to ethical values, and respecting the rule of law

The Council is committed to:

Behaving with Integrity

- Ensuring members and officers behave with integrity and lead as a culture where acting in the public interest is visibly and consistently demonstrated thereby protecting the reputation of the organisation.
- Ensuring members take the lead in establishing specific standard operating principles or values for the organisation and its staff and that they are communicated and understood. These should build on the Seven Principles of Public Life (The Nolan Principles).
- Leading by example and using these standard operating principles or values as a framework for decision making and other actions.
- Demonstrating, communicating and embedding the standard operating principles or values through appropriate policies and processes which are reviewed on a regular basis to ensure they are operating effectively.

Demonstrating strong commitment and ethical values

- Seeking to establish, monitor and maintain the organisation's ethical standards and performance.

- Underpinning personal behaviour with ethical values and ensuring they permeate all aspects of the organisation's culture and operation.
- Developing and maintaining robust policies and procedures which place emphasis on agreed ethical values.
- Ensuring that external providers of services on behalf of the organisation are required to act with integrity and in compliance with high ethical standards expected by the organisation.

Respecting the rule of law

- Ensuring members and staff demonstrate a strong commitment to the rule of the law as well as adhering to relevant laws and regulations.
- Creating the conditions to ensure that the statutory officers, other key post holders and members are able to fulfil their responsibilities in accordance with legislative and regulatory requirements.
- Striving to optimise the use of the full powers available for the benefit of citizens, communities and other stakeholders.
- Dealing with breaches of legal and regulatory provisions effectively and ensuring corruption and misuse of power are dealt with effectively.

Principle B – Ensuring openness and comprehensive stakeholder engagement

The Council is committed to:

Openness

Ensuring an open culture through demonstrating, documenting and communicating the organisation's commitment to openness

- Making decisions that are open about actions, plans, resource use, forecasts, outputs and outcomes. The presumption is for openness. If that is not the case, a justification for the reasoning for keeping a decision confidential should be provided.
- Providing clear reasoning and evidence for decisions in both public records and explanations to stakeholders and being explicit about the criteria, rationale and considerations used. In due course, ensuring that the impact and consequences of those decisions are clear.
- Using formal and informal consultation and engagement to determine the most appropriate and effective interventions/ courses of action.

Engaging comprehensively with institutional stakeholders

- Effectively engaging with institutional stakeholders to ensure that the purpose, objectives and intended outcomes for each stakeholder relationship are clear so that outcomes are achieved successfully and sustainably.
- Developing formal and informal partnerships to allow for resources to be used more efficiently and outcomes achieved more effectively.
- Ensuring that partnerships are based on trust, a shared commitment to change, a culture that promotes and accepts challenge among partners and that the added value of partnership working is explicit.

Engaging stakeholders effectively, including individual citizens and service users

- Establishing a clear policy on the type of issues that the organisation will meaningfully consult with or involve individual citizens, service users and other stakeholders to ensure that service (or other) provision is contributing towards the achievement of intended outcomes.
- Ensuring that communication methods are effective, and that members and officers are clear about their roles with regard to community engagement
- Encouraging, collecting and evaluating the views and experiences of communities, citizens, service users and organisations of different backgrounds including reference to future needs.
- Implementing effective feedback mechanisms in order to demonstrate how their views have been taken into account.
- Balancing feedback from more active stakeholder groups with other stakeholder groups to ensure inclusivity.
- Taking account of the interests of future generations of tax payers and service users.

Principle C – Defining outcomes in terms of sustainable economic, social, and environmental benefits

The Council is committed to:

Defining outcomes

- Having a clear vision which is an agreed formal statement of the organisation's purpose and intended outcomes containing appropriate performance indicators, which provides the basis for the organisation's overall strategy, planning and other decisions.
- Specifying the intended impact on, or changes for, stakeholders including citizens and service users. It could be immediately or over the course of a year or longer.
- Delivering defined outcomes on a sustainable basis within the resources that will be available.
- Identifying and managing risks to the achievement of outcomes.
- Managing service users expectations effectively with regard to determining priorities and making the best use of the resources available.

Sustainable economic, social and environmental benefits

- Considering and balancing the combined economic, social and environmental impact of policies, plans and decisions when taking decisions about service provision.
- Taking a longer-term view with regard to decision making, taking account of risk and acting transparently where there are potential conflicts between the organisation's intended outcomes and short-term factors such as the political cycle or financial constraints.
- Ensuring fair access to services.
- Determining the wider public interest associated with balancing conflicting interests between achieving the various economic, social and environmental benefits, through consultation where possible, in order to ensure appropriate trade-offs.

Principle D – Determining the interventions necessary to optimise the achievement of the intended outcomes

The Council is committed to:

Determining interventions

- Ensuring decision makers receive objective and rigorous analysis of a variety of options indicating how intended outcomes would be achieved and including the risks associated with those options. Therefore, ensuring best value is achieved however services are provided.
- Considering feedback from citizens and service users when making decisions about service improvements or where services are no longer required in order to prioritise competing demands within limited resources available including people, skills, land and assets and bearing in mind future impacts.

Planning interventions

- Establishing and implementing robust planning and control cycles that cover strategic and operational plans, priorities and targets.
- Engaging with internal and external stakeholders in determining how services and other courses of action should be planned and delivered.
- Considering and monitoring risks facing each partner when working collaboratively including shared risks.
- Ensuring arrangements are flexible and agile so that the mechanisms for delivering outputs can be adapted to changing circumstances.
- Establishing appropriate key performance indicators (KPIs) as part of the planning process in order to identify how the performance of services and projects is to be measured.
- Ensuring capacity exists to generate the information required to review service quality regularly.
- Preparing budgets in accordance with organisational objectives, strategies and the medium term financial plan Informing medium and long term resource planning by drawing up realistic estimates of revenue and capital expenditure aimed at developing a sustainable funding strategy.

Optimising achievement of intended outcomes

- Ensuring the medium term financial strategy integrates and balances service priorities, affordability and other resource constraints.
- Ensuring the budgeting process is all-inclusive, taking into account the full cost of operations over the medium and longer term.
- Ensuring the medium term financial strategy sets the context for ongoing decisions on significant delivery issues or responses to changes in the external environment that may arise during the budgetary period in order for outcomes to be achieved while optimising resource usage.
- Ensuring the achievement of 'social value' through service planning and commissioning.

Principle E – Developing the entity's capacity, including the capability of its leadership and the individuals within it

The Council is committed to:

Developing the entity's capacity

- Reviewing operations, performance use of assets on a regular basis to ensure their continuing effectiveness.
- Improving resource use through appropriate application of techniques such as benchmarking and other options in order to determine how the authority's resources are allocated so that outcomes are achieved effectively and efficiently.
- Recognising the benefits of partnerships and collaborative working where added value can be achieved.

- Developing and maintaining an effective workforce plan to enhance the strategic allocation of resources.

Developing the capability of the entity’s leadership and other individuals

- Developing protocols to ensure that elected and appointed leaders negotiate with each other regarding their respective roles early on in the relationship and that a shared understanding of roles and objectives is maintained.
- Publishing a statement that specifies the types of decisions that are delegated and those reserved for the collective decision making of the governing body.
- Ensuring the leader and the chief executive have clearly defined and distinctive leadership roles within a structure whereby the chief executive leads the authority in implementing strategy and managing the delivery of services and other outputs set by members and each provides a check and a balance for each other’s authority.
- Developing the capabilities of members and senior management to achieve effective shared leadership and to enable the organisation to respond successfully to changing legal and policy demands as well as economic, political and environmental changes and risks by:
 - ensuring members and staff have access to appropriate induction tailored to their role and that ongoing training and development matching individual and organisational requirements is available and encouraged.
 - ensuring members and officers have the appropriate skills, knowledge, resources and support to fulfil their roles and responsibilities and ensuring that they are able to update their knowledge on a continuing basis.
 - ensuring personal, organisational and system-wide development through shared learning, including lessons learnt from governance weaknesses both internal and external.
- Ensuring that there are structures in place to encourage public participation.
- Taking steps to consider the leadership’s own effectiveness and ensuring leaders are open to constructive feedback from peer review and inspections.
- Holding staff to account through regular performance reviews which take account of training or development needs Ensuring arrangements are in place to maintain the health and wellbeing of the workforce and support individuals in maintaining their own physical and mental wellbeing.

Principle F – Managing risks and performance through robust internal control and strong public financial management

The Council is committed to:

Managing risk

- Recognising that risk management is an integral part of all activities and must be considered in all aspects of decision making.

- Implementing robust and integrated risk management arrangements and ensuring that they are working effectively.
- Ensuring that responsibilities for managing individual risks are clearly allocated.

Managing performance

- Monitoring service delivery effectively including planning, specification, execution and independent post implementation review.
- Making decisions based on relevant, clear objective analysis and advice pointing out the implications and risks inherent in the organisation's financial, social and environmental position and outlook.
- Ensuring an effective scrutiny or oversight function is in place which encourages constructive challenge and debate on policies and objectives before, during and after decisions are made thereby enhancing the organisation's performance and that of any organisation for which it is responsible (OR, for a committee system).
- Encouraging effective and constructive challenge and debate on policies and objectives to support balanced and effective decision making.
- Providing members and senior management with regular reports on service delivery plans and on progress towards outcome achievement.
- Ensuring there is consistency between specification stages (such as budgets) and post implementation reporting (e.g. financial statements).

Robust internal control

- Aligning the risk management strategy and policies on internal control with achieving the objectives.
- Evaluating and monitoring the authority's risk management and internal control on a regular basis.
- Ensuring effective counter fraud and anti-corruption arrangements are in place.
- Ensuring additional assurance on the overall adequacy and effectiveness of the framework of governance, risk management and control is provided by the internal auditor.
- Ensuring an effective audit committee or equivalent group or function which is independent of the executive and accountable to the governing body: provides a further source of assurance regarding arrangements for managing risk and maintaining an effective control environment that its recommendations are listened to and acted upon.

Managing Data

- Ensuring effective arrangements are in place for the safe collections, storage, use and sharing of data, including processes to safeguard personal data.
- Ensuring effective arrangements are in place and operating effectively when sharing data with other bodies.
- Reviewing and auditing regularly the quality and accuracy of data used in decision making and performance monitoring.

Strong Public Financial Management

- Ensuring financial management supports both long term achievement of outcomes and short-term financial and operation performance.
- Ensuring well-developed financial management is integral at all levels of planning control and control, including management of financial risks and controls.

Principle G – Implementing good practices in transparency, reporting, and audit to deliver effective accountability

The Council is committed to:

Implementing good practice in transparency

- Writing and communicating reports for the public and other stakeholders in an understandable style appropriate to the intended audience and ensuring that they are easy to access and interrogate.
- Striking a balance between providing the right amount of information to satisfy transparency demands and enhance public scrutiny while not being too onerous to provide and for users to understand.

Implementing good practice in reporting

- Reporting at least annually on performance, value for money and the stewardship of its resources.
- Ensuring members and senior management own the results.
- Ensuring robust arrangements for assessing the extent to which the principles contained in the Framework have been applied and publishing the results on this assessment including an action plan for improvement and evidence to demonstrate good governance (annual governance statement).
- Ensuring that the Framework is applied to jointly managed or shared service organisations as appropriate.
- Ensuring the performance information that accompanies the financial statements is prepared on a consistent and timely basis and the statements allow for comparison with other similar organisations.

Assurance and effective accountability

- Ensuring that recommendations for corrective action made by external audit are acted upon.
- Ensuring an effective internal audit service with direct access to Audit and Governance Committee members is in place which provides assurance with regard to governance arrangements and recommendations are acted upon.
- Welcoming peer challenge, reviews and inspections from regulatory bodies and implementing recommendations.
- Gaining assurance on risks associated with delivering services through third parties and that this is evidenced in the annual governance statement.
- Ensuring that when working in partnership, arrangements for accountability are clear and that the need for wider public accountability has been recognised and met.

NORTH WEST LEICESTERSHIRE DISTRICT COUNCIL

AUDIT AND GOVERNANCE COMMITTEE – WEDNESDAY
26 JULY 2023



Title of Report	UPDATE ON THE IMPLEMENTATION OF THE CIPFA POSITION STATEMENT: AUDIT COMMITTEES IN LOCAL AUTHORITIES AND POLICE 2022	
Presented by	Kerry Beavis Audit Manager	
Background Papers	CIPFA Position Statement: Audit Committees in Local Authorities and Police 2022 Audit committees: practical guidance for local authorities and police (to be circulated)	Public Report: Yes
Purpose of Report	To update members on the initial meeting of the working group and the work which is ongoing to ensure that the Council complies with CIPFA's Position Statement: Audit Committees in Local Authorities, as agreed at the Audit & Governance committee meeting on 26 April 2023.	
Recommendations	THAT THE AUDIT AND GOVERNANCE COMMITTEE 1. NOTES THE REPORT. 2. AGREE THE PROCESS FOR THE RECRUITMENT OF INDEPENDENT MEMBERS TO THE COMMITTEE. 3. AGREE THE PROPOSED ACTION PLAN DETAILED IN APPENDIX D	

1. INTRODUCTION

- 1.1 At its meeting on 26 April 2023, the Audit & Governance Committee considered the Chartered Institute of Public Finance & Accountancy (CIPFA) updated [Position Statement: Audit Committees in Local Authorities and Police 2022](#)
- 1.2 The Committee were advised that the Guidance continued to include a strong focus on the factors that supported improvement in the working of audit committees. This included the knowledge and skills that Audit & Governance Committee members require and an emphasis on where the Committee can add value. It also provided practical support in evaluating the existing Committee and planning any improvements identified.
- 1.3 In accordance with the decision of the committee in April, a cross party working group was formed, comprising Cllrs Sutton, Everitt, Moulton, and Simmons, supported by the Head of Legal & Support Services and the Audit Manager. The terms of reference of the group are attached at appendix A.

2. SELF-ASSESSMENT PROCESS

- 2.1 The knowledge and skills questionnaire was distributed to all Committee members for completion, to identify gaps in knowledge and skills. A distinction is made between core areas of knowledge that all Audit & Corporate Governance Committee members should seek to acquire and a range of specialisms that can add value to the Committee.
- 2.2 The group reviewed the outcomes of the self-assessment, discussed the requirement for two co-opted independent member and the requirement to meet the position statement to the best of the Committee's ability.

3. KEY FINDINGS AND

- 3.1 Five responses to the questionnaire were received. The working group reviewed these responses. The level of responses received is broadly considered representative of the views of the Committee as a whole.
- 3.2 A summary of responses received are attached at Appendix B.
- 3.3 The main areas identified for training as part of the member induction process and on an ongoing basis are:
 - Organisational Knowledge
 - Audit Committee Role and Functions
 - Governance
 - Internal Audit
 - Financial Management and Financial Reporting
 - External Audit

- Risk Management
- Counter Fraud
- Values of good governance
- Treasury Management

3.4 It was agreed at the working group that further and ongoing training is required to support members with their responsibilities within the Audit & Governance Committee, with a training plan to be developed at the working group meeting in September.

4. OUTCOMES

4.1 The working group also agreed that co-opted independent members be appointed to the committee to assist with any knowledge and skills gaps with the appointment process to be agreed by the committee.

4.2 A person specification/ job description be developed, this is included at Appendix C for approval by the committee.

4.3 In addition to considering the above matters, the group agreed that they would meet in September and March to undertake further work to comply with the Position Statement, in particular a review of the work programme of the committee to ensure it aligns with the Position Statement requirements, and to develop the annual report of the Committee.

3.6 Following the working group meeting the Audit Manager has developed an action plan, Appendix D

CIPFA's Position Statement: Audit Committees in Local Authorities 2022

Officer/Cross-Party Working Group

Terms of Reference

Role

To assist with the process of implementing the good practice recommended by CIPFA's Position Statement in particular:

- the development of a job description for independent members of the committee and the appointment of such members.
- a review of the skills and knowledge of the members of the committee and the development of a forward training plan.
- the annual review on how the committee has complied with the position statement, discharged its responsibilities, and an assessment of its performance.

Who has voting rights on the recommendations?

Only elected Members have voting rights.

Members of the Cross-Party Working Group

Cllr Sutton
Cllr Everitt
Cllr Moulton
Cllr Simmons

What is expected of officers of the Cross-party Working Group?

- Provide professional advice, support, and guidance, throughout the piece of work.
- Ensure effective administration of the working group including provision of agendas and minutes.

Officers of the Cross-party Working Group

- Kerry Beavis, Internal Audit Manager – Lead Officer.
- Elizabeth Warhurst, Head of Legal and Support Services and MO.

How often will the Group meet?

To be considered and agreed by the Group – may be workload dependent. Meetings to be via MS Teams or in person as appropriate for the relevant action topic.

AUDIT & GOVERNANCE COMMITTEE MEMBERS – KNOWLEDGE AND SKILLS FRAMEWORK

Core Areas of Knowledge

Knowledge Area	Details of core knowledge required	How the audit committee member is able to apply the knowledge	Overall assessment of skills/knowledge (1-5, 1 being minimal and 5 being strong)				
			1	2	3	4	5
Organisational knowledge	<ul style="list-style-type: none"> An overview of the authority’s governance structures and decision-making processes. Knowledge of the organisational objectives and major functions of the authority. 	<ul style="list-style-type: none"> This knowledge will be core to most of the audit committee’s activities, including the Annual Governance Statement (AGS) review, internal and external audit reports, and risk registers. 	2		2	1	
Audit committee role and functions	<ul style="list-style-type: none"> An understanding of the audit committee’s role and place within the governance structures. Familiarity with the committee’s terms of reference and accountability arrangements. Knowledge of the purpose and role of the audit committee. 	<ul style="list-style-type: none"> This knowledge will enable the audit committee to prioritise its work to ensure it discharges its responsibilities under its terms of reference and to avoid overlapping the work of others. It will help the committee undertake a self-assessment and prepare its annual report. 	1	2	1	1	
Governance	<ul style="list-style-type: none"> Knowledge of the seven principles as outlined in Delivering Good Governance in Local Government: Framework (CIPFA/Solace, 2016). The requirements of the AGS. How the principles of governance are implemented locally as set out in the local code of governance. 	<ul style="list-style-type: none"> The committee will review the local code of governance and consider how governance arrangements align to the principles in the Framework. The committee will plan the assurances it is to receive to adequately support the AGS. The committee will review the AGS and consider how the authority is meeting the principles of good governance. The committee will receive audit reports and information on risks relating to governance. 	2	2		1	
Internal audit	<ul style="list-style-type: none"> An awareness of the key principles of the Public Sector Internal Audit Standards (PSIAS) and the Local Government Application Note (LGAN). Knowledge of the arrangements for delivery of the internal audit service in the authority and the charter. How the role of the head of internal audit is fulfilled. Details of the most recent external assessment and level of conformance with the standards. Internal audit’s strategy, plan, and most recent annual opinion 	<ul style="list-style-type: none"> The audit committee has oversight of the internal audit function and will monitor its adherence to professional internal audit standards. The audit committee will review the assurances from internal audit work and will review the risk-based audit plan. The committee will also receive the annual report, including an opinion and information on conformance with professional standards. In relying on the work of internal audit, the committee will need to be confident that professional standards are being followed. 	1	1	1	1	1

		<ul style="list-style-type: none"> The audit committee chair is likely to be interviewed as part of the external quality assessment, and the committee will receive the outcome of the assessment and action plan. 					
Financial management and financial reporting	<ul style="list-style-type: none"> Awareness of the financial statements that a local authority must produce and the principles it must follow to produce them. An understanding of good financial management practice as set out in the CIPFA Financial Management Code (FM Code) and the level of compliance with it. Knowledge of how the organisation meets the requirements of the role of the Chief Finance Officer (CFO) as required by The Role of the Chief Financial Officer in Local Government (CIPFA, 2016). An overview of the principal financial risks the authority faces. 	<ul style="list-style-type: none"> Reviewing the financial statements prior to publication, asking questions. Receiving the external audit report and opinion on the financial audit. Reviewing both external and internal audit recommendations relating to financial management and controls. The audit committee should consider compliance with the FM Code and the role of the CFO and how this is met when reviewing the AGS. 	1	1		3	
212 External audit	<ul style="list-style-type: none"> Knowledge of the role and functions of the external auditor and who currently undertakes this role. Knowledge of the key reports and assurances that external audit will provide. Familiarity with the auditor's most recent plan and the opinion reports. Knowledge about arrangements for the appointment of auditors and quality management undertaken. 	<ul style="list-style-type: none"> The audit committee will meet with the external auditor regularly and receive their reports and opinions. Monitoring external audit recommendations and maximising the benefit from the audit process. The audit committee should monitor the relationship between the external auditor and the authority and support the delivery of an effective service. 	1	2		2	
Risk management	<ul style="list-style-type: none"> Understanding of the principles of risk management, including how it supports good governance and decision making. Knowledge of the risk management policy and strategy of the organisation. Understanding of risk governance arrangements, including the role of members and of the audit committee. Knowledge of the current risk maturity of the organisation and any key areas of improvement. 	<ul style="list-style-type: none"> In reviewing the AGS, the committee will consider the robustness of the authority's risk management arrangements. Awareness of the major risks the authority faces is necessary to support the review of several audit committee agenda items, including the risk-based internal audit plan, external audit plans and the explanatory foreword of the accounts. Typically, risk registers will be used to inform the committee. The committee should also review reports and action plans to develop the application of risk management practice 	2		1	2	
Counter fraud	<ul style="list-style-type: none"> An understanding of the main areas of fraud and corruption risk that the organisation is exposed to. Knowledge of the principles of good fraud risk management practice in accordance with the Code of Practice on Managing the Risk of Fraud and Corruption (CIPFA, 2014). Knowledge of the organisation's arrangements for tackling fraud. 	<ul style="list-style-type: none"> Knowledge of fraud risks and good fraud risk management practice will be helpful when the committee reviews the organisation's fraud strategy and receives reports on the effectiveness of that strategy. An assessment of arrangements should support the AGS, and knowledge of good fraud risk management practice will support the audit committee member in reviewing that assessment. 	1	1	1	2	

Values of good governance	<ul style="list-style-type: none"> • Knowledge of the Seven Principles of Public Life. • Knowledge of the authority's key arrangements to uphold ethical standards for both members and staff (eg code of conduct). • Knowledge of the whistleblowing arrangements in the authority. 	<ul style="list-style-type: none"> • The audit committee member will draw on this knowledge when reviewing governance issues and the AGS. • Oversight of the effectiveness of whistleblowing will be considered as part of the AGS. The audit committee member should know to whom concerns should be reported. 	1	2	1	1	
Treasury management	<ul style="list-style-type: none"> • Effective Scrutiny of Treasury Management is an assessment tool for reviewing the arrangements for undertaking scrutiny of treasury management. The key knowledge areas identified are: <ul style="list-style-type: none"> – regulatory requirements – treasury risks – the organisation's treasury management strategy – the organisation's policies and procedures in relation to treasury management. 	<ul style="list-style-type: none"> • Core knowledge on treasury management is essential for the committee undertaking the role of scrutiny. 	1	2	1	1	

Core Skills

Skills	Key Elements	How the audit committee member is able to apply the skill	Overall assessment of skills/knowledge (1-5, 1 being minimal and 5 being strong)				
			1	2	3	4	5
Strategic thinking and understanding of materiality	Able to focus on material issues and the overall position rather than being side tracked by detail.	When reviewing audit reports, findings will include areas of higher risk or materiality to the organisation but may also highlight more minor errors or control failures. The audit committee member will need to pitch their review at an appropriate level to avoid spending too much time on detail.		2	2	1	
Questioning and constructive challenge	Able to frame questions that draw out relevant facts and explanations, challenging performance and seeking explanations while avoiding hostility or grandstanding.	The audit committee will review reports and recommendations to address weaknesses in internal control. The audit committee member will seek to understand the reasons for weaknesses and ensure a solution is found.		1	2	1	1
Focus on improvement	Ensuring there is a clear plan of action and allocation of responsibility.	The audit committee's outcome will be to secure improvements to the governance, risk management or control of the organisation, including clearly defined actions and responsibilities. Where errors or control failures have occurred, the audit committee should seek assurances that appropriate action has been taken.		2	1	1	1
Able to balance practicality against theory	Able to understand the practical implications of recommendations to understand how they might work in practice.	The audit committee should seek assurances that planned actions are practical and realistic.		1	2	2	
Clear communication skills and focus on the needs of users	Support the use of plain English in communications, avoiding jargon, acronyms, etc	The audit committee will seek to ensure that external documents such as the AGS and the narrative report in the accounts are well written for a non-expert audience.	1	1	2	1	
Objectivity	Evaluate information based on evidence presented, avoiding bias or subjectivity.	The audit committee will receive assurance reports and review risk registers. There may be differences of opinion about the significance of risk and the appropriate control responses, and the committee member will need to weigh up differing views.		1	2	1	1
Meeting management skills	Chair the meetings effectively: summarise issues raised, ensure all participants can contribute, and focus on the outcome and actions from the meeting.	These skills are essential for the audit committee chair to help ensure that meetings stay on track and address the items on the agenda. The skills are desirable for all other members.	1	1	2	1	



APPOINTMENT OF INDEPENDENT MEMBER FOR AUDIT & GOVERNANCE COMMITTEE

North West Leicestershire District Council is committed to the highest standards of corporate governance, and our Audit & Governance Committee is a key part of ensuring that we meet those standards. The Council is currently looking to appoint an independent co-opted member to the Committee, to become a part of its work in promoting excellence in governance, risk management, financial reporting and counter fraud.

Independent Members will be expected to actively participate in meetings of the Audit & Governance Committee and demonstrate independence, integrity, objectivity and impartiality in their decision-making. As part of this rewarding role, they will support the Council's Audit & Governance Committee in providing independent assurance to the members of North West Leicestershire District Council, and its wider citizens and stakeholders.

Independent Members are non-voting members of the Committee, who assist in overseeing internal and external audit arrangements, reviewing and scrutinising financial statements, and reviewing and assessing the governance, risk management and control of the authority.

The terms of reference for the Audit & Governance Committee can be found in the Council's Constitution which is published on our website.

The Independent Member will be appointed for a four-year period. We have a preference for candidates who have either lived or worked within the district or are otherwise familiar with the district.

Successful candidates will be expected to attend approximately five Committee meetings per year, which take place at Stenson House, Whitwick Road, Coalville. They will also need to commit sufficient time to read Committee papers in advance of these meetings, liaise with the Chair and to undertake training alongside the other Committee members.

Independence

a) A person can only be an independent person if that person:

- Is not a member, co-opted member or officer of the authority, or has been within the last 5 years;
- Is not a member, co-opted member or officer of a parish council of which the authority is the principal authority, or has been within the last 5 years;
- Is not a relative or close friend, of a person within (a) and (b);
- Has submitted an application form in response to an advert for the position at the authority;

- In addition to be eligible for appointment, a person must not be disqualified from holding office as a Member of the Council. Accordingly, any person who is recommended for appointment will be required to confirm that he/she is not disqualified.

b) A 'relative' means:

- a) the other person's spouse or civil partner;
- b) living with the other person as husband and wife or as if they were civil partners;
- c) a grandparent of the other person;
- d) a lineal descendant of a grandparent of the other person;
- e) a parent, sibling or child of a person within paragraph (a) or (b);
- f) the spouse or civil partner of a person within paragraph (c), (d) or (e), or
- g) living with a person within paragraph (c), (d) or (e) as husband and wife or as if they were civil partners.

Selection Criteria

The ideal candidate for the position will:

1. Be willing and able to commit the necessary time to the role;
2. Have up to date skills, knowledge and experience within at least one of the fields covered within Audit & Governance Committee, i.e. internal audit, risk management, governance, accounting, anti-fraud and corruption;
3. Have good interpersonal skills, including good communication skills both written and oral and the ability to co-operate with others in a committee setting.
4. Have independence of mind, objectivity and impartiality.
5. Make independent, proactive, and proportionate contributions and listen to, and balance, advice;
6. Have a commitment to the general principles governing the conduct of Councillors generally and work to high behavioural standards, demonstrating honesty, probity and integrity;
7. Not be a serving local government officer or councillor;
8. Have no personal, legal or contractual relationship with North West Leicestershire District Council (including employees or Members or former staff), or any other relationship / activity which might represent a conflict of interest or perceived conflict of interest.

Desirable additional criteria are:

1. A suitable professional or management qualification (in internal audit, risk management, governance, accounting, or other relevant discipline).
2. An understanding of the complexity of issues surrounding audit, risk management, governance, and finance in local government.
3. An understanding of the Council's vision, priorities, and objectives.
4. An ability to understand complex situations and reports, as well as the statutory background to those reports, and ask appropriate questions of officers.

5. Have a broad range of experience, possibly in public, private, voluntary or charitable sector employment or service including self-employed, employed and voluntary positions.
6. Promotes the work of the Audit & Governance Committee and areas falling under its terms of reference.
7. Have a connection with North West Leicestershire District, e.g. resident, workplace, own a business etc.

Remuneration

Co-opted independent members do not receive an allowance but are entitled to claim for reasonable travelling and subsistence expenses in undertaking their role.

Means of assessment

Application form and by interview.

If you are interested in becoming an Independent Member of the Audit & Governance Committee, we would be delighted to hear from you. Please apply by completing the application form, outlining why you are interested in this opportunity and how your skills and experience relate to the role to: XXXXXXXXX

Appointment of candidates will be strictly in accordance with the selection criteria and desirable additional criteria outlined in this pack and will be based on the information contained in your application only, as supported by references. It is suggested therefore that you include information on how you meet the criteria.

Your application will be acknowledged, and you will be advised as to whether you have been selected for interview or not in due course.

Please note that interviews for the role will be held on the XXXXXXXX at XXXXXXXXXX

SUMMARY ACTION PLAN

Ref	Action	Assigned to	Timescale
1	Interviews for co-opted independent members.	Cllr Moulton, Cllr Sutton, Audit Manager.	September 2023
2	Training plan to be developed to ensure all committee members have a reasonable level of knowledge in the relevant areas.	Working Group, with assistance from Director of Resources, Head of Legal and Support Services, Head of Finance, Audit Manager	September 2023
3	Review of the Self-Assessment of Good Practice to then consider areas of weakness and improvements required to meet the key principles as set out in the Position Statement.	Working Group with assistance from Head of Legal & Support Services, Audit Manager	September 2023
4	Review of the annual work plan of the audit committee to ensure that it reflects the position statement.	Working Group with assistance from Head of Legal & Support Services, Audit Manager	September 2023
5	Approval of the appointment of the co-opted independent members.	Audit & Governance Committee	October 2023
6	The Audit & Governance Committee should produce an annual report on how they complied with the position statement, discharged its responsibilities, and include an assessment of its performance.	Working Group with assistance from Head of Legal & Support Services, Audit Manager and input from all committee members.	To be completed for agreement by the Audit & Governance Committee at the April 2024 meeting
7	Annual Report to be presented at full Council	Chair of Audit & Governance Committee	May 2024

Potential Training Topics

- Reviewing and approving the Annual Statement of Accounts and Annual Governance Statement;
- Reviewing the findings of both Internal and External examinations and ensuring that appropriate action is taken to remedy weaknesses identifies;
- Monitoring the effective development and operation of risk management;
- Reviewing and monitoring governance arrangements/ Good Governance Framework.
- Fraud Awareness

This page is intentionally left blank

NORTH WEST LEICESTERSHIRE DISTRICT COUNCIL



AUDIT AND GOVERNANCE COMMITTEE WEDNESDAY, 26
JULY 2023

Title of Report	INTERNAL AUDIT PROGRESS REPORT	
Presented by	Kerry Beavis Audit Manager	
Background Papers	Public Sector Internal Audit Standards Internal Audit Plan 2023/24	Public Report: Yes
Purpose of Report	To inform the Committee of progress against the Internal Audit plan for 2023/24 and to highlight any incidences of significant control failings or weaknesses that have been identified.	
Recommendations	THE AUDIT AND GOVERNANCE COMMITTEE NOTE THE REPORT.	

1.0 BACKGROUND

- 1.1. The Public Sector Internal Audit Standards require the Authority's Audit Committee to approve the audit plan and monitor progress against it. The Standards state that the Committee should receive periodic reports on the work of internal audit.
- 1.2 The Audit and Governance Committee approved the 2023/24 Audit Plan on 26 April 2023. The Committee receives quarterly progress reports.

2.0 PROGRESS REPORT

- 2.1 The Internal Audit Progress Report for the period 1 April 2023 to 30 June 2023 (Q1) is attached at Appendix 1.

Policies and other considerations, as appropriate	
Council Priorities:	An effective internal audit service supports all council priorities.
Policy Considerations:	None.
Safeguarding:	None.
Equalities/Diversity:	None.
Customer Impact:	None.
Economic and Social Impact:	None.
Environment and Climate Change:	None.
Consultation/Community Engagement:	None.
Risks:	There are no specific risks associated with this report.
Officer Contact	<p>Kerry Beavis Audit Manager Kerry.beavis@nwleicestershire.gov.uk</p> <p>Elizabeth Warhurst Head of Legal and Support Services elizabeth.warhurst@nwleicestershire.gov.uk</p>



INTERNAL AUDIT SHARED SERVICE

North West Leicestershire District Council

Internal Audit Progress Report 2023/24 Q1

1. Introduction

1.1. Internal Audit is provided through a shared service arrangement led by North West Leicestershire District Council and delivered to Blaby District Council and Charnwood Borough Council. The assurances received through the Internal Audit programme are a key element of the assurance framework required to inform the Annual Governance Statement. The purpose of this report is to highlight progress against the 2023/24 Internal Audit Plan up to 30 June 2023.

2. Internal Audit Plan Update

2.1. Work on the 2023/24 audit plan has commenced. The 2023/24 audit plan is included at Appendix A for information. The audits due to take place in Q2 are:

- Housing Repairs
- Housing Planned Maintenance
- Procurement & Contract Management
- Asbestos Management

2.2. Since the last update report five final reports have been issued from the 2022/23 audit plan, this concludes the audit work for 2022/23. The executive summaries are included at Appendix B.

3. Internal Audit Recommendations

3.1. Internal Audit monitor and follow up critical, high and medium priority recommendations. Further details of overdue and extended recommendations are detailed in Appendix C for information.

Year	Not Due		Extended		Overdue	
	High	Medium	High	Medium	High	Medium
21/22	-	-	10	3	-	-
22/23	27	20	-	-	-	-

4. Internal Audit Performance Indicators

4.1. Progress against the agreed Internal Audit performance targets is documented in Appendix D.

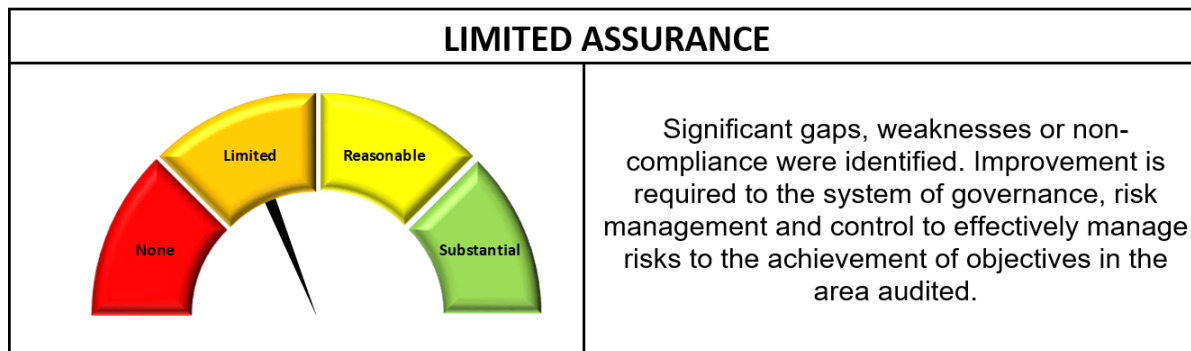
2023/24 AUDIT PLAN AS AT 30 JUNE 2023

Audit Area	Type	Planned Days	Actual Days	Status	Assurance Level	Recommendations				Comments
						C	H	M	L	
Housing Repairs Q1	Audit	10		Q1						
Housing Repairs Q2	Audit	10		Q2						
Housing Repairs Q3	Audit	10		Q3						
Housing Repairs Q4	Audit	10		Q4						
Housing Planned Maintenance Q1	Audit	10		Q1						
Housing Planned Maintenance Q2	Audit	10		Q2						
Housing Planned Maintenance Q3	Audit	10		Q3						
Housing Planned Maintenance Q4	Audit	10		Q4						
Asbestos Management	Audit	10		Q2						
HMO/ Selective Licensing	Audit	10		Q4						
Safeguarding	Audit	8	3.5	In Progress						
Transport Management & Operating Licensing	Audit	8		Q4						
Tree Stock Management	Audit	6		Q3						
Protect Duty	Audit	8		Q4						
New finance system	Advisory/ Testing	10		Q1/2/3						
Key financial systems	Audit	52		Q1/2/3/4						
Workforce Planning	Audit	10		Q2						
IT Asset Management	Audit	10	4	In Progress						
Remote Support & Data Exchange	IT Audit Contractor	IT Contractor		TBA						
Cyber Security	IT Audit Contractor	IT Contractor		TBA						

Corporate Policy Management	Audit / Data analysis	10	1							
Capital Programme Management	Audit	10		Q1 & Q4						
Transformation Projects	Advisory	5		As required						
Climate Change Strategy	Audit	10		Q4						
Procurement & Contract Management	Audit	10		Q2						
Grant Assurance	Assurance		6	As required						

SUMMARY OF FINAL AUDIT REPORTS ISSUED BETWEEN 1 APRIL & 30 JUNE 2023

PAYROLL – 2022/23

**Key Findings**

227

Areas of positive assurance identified during the audit:

- Regular reconciliations are carried out between the payroll system, general ledger, bank accounts and any suspense accounts.
- Payroll is reviewed for accuracy prior to authorisation and payment.

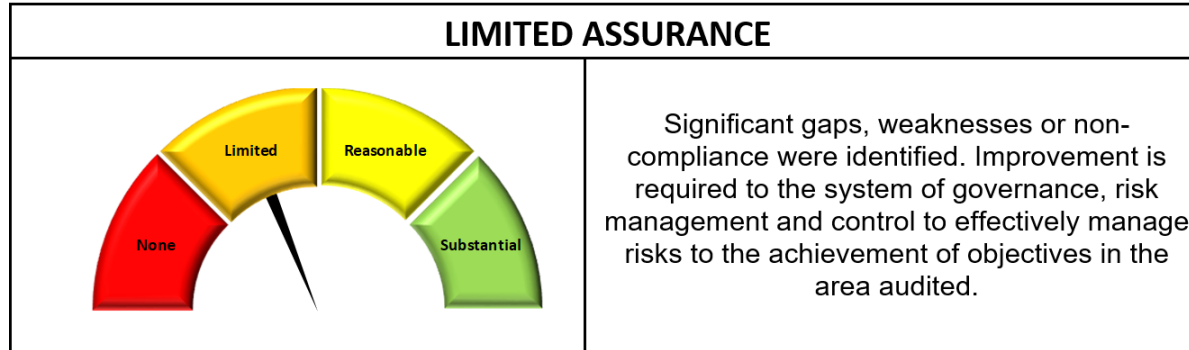
The main areas identified for improvement are:

- Cover arrangements for the HR Analyst.
- Segregation of duty between HR and Payroll functions.
- Testing of the accuracy of payroll prior to year-end following the annual updating of tax, national insurance rates and tax code changes.
- Annual review and confirmation of the establishment to iTrent.
- System Administrator and HR Analyst access to iTrent.
- Regular review of access to iTrent.

Recommendation	Priority	Response/Agreed Action	Officer Responsible	Implementation Date
1. A review of the roles carried out between HR Administration, HR Payroll and Finance Payroll should be carried out to ensure, adequate separation of duties exist between HR (staffing), payroll (preparation) and payroll (payment).	High	Agree – will need to look at roles of staff and how to implement to ensure adequate separation of duties.	Head of Finance, Head of HR and Organisational Development	April 2024
2. A regular review of the iTrent audit log is carried out by an independent officer to ensure functions are appropriate to the officer.	High	Agree – appropriate audit log to be sourced, possibly reviewed by Senior HR Advisors.	Head of HR and Organisational Development.	December 2023
3. Consideration should be given to providing training to a member of the Human Resources Team to ensure business continuity in the event of the absence of the HR Analyst.	Medium	Agree – training to be provided to a member of the HR Team but may require additional resource.	Head of HR and Organisational Development.	December 2023
4. Sample testing should be undertaken when changes to standing data occur to confirm they have been correctly applied.	High	Agree – sample checking to be undertaken and evidence retained.	Payroll Officer / HR Analyst	December 2023
5. On, at least, an annual basis an establishment report from iTrent should be run and issued to Heads of Service / Managers to confirm the accuracy of the report. The report should include all staff, vacancies, hours worked, contractual basis, salary and salary point. Checks should be documented and once completed should be returned to HR to action any items identified and to retain as evidence of checks being undertaken.	High	Agree – report to be obtained from iTrent and issued on an annual basis.	Head of HR and Organisational Development	March 2024
6. A review of the payroll checking process is carried out to eliminate duplication, reduce the risk of fraud and ensure independence in the review and checking of the monthly payroll.	High	Agree – current payroll checks to be reviewed and revised.	Exchequer Services Team Leader and Head of HR and Organisational Development	December 2023

7. A full review of user access is carried out, in particular System Administrator access should be reviewed, and the number reduced.	High	Agree – access to be reviewed and removed where no longer required.	Head of HR and Organisational Development	December 2023
8. A review of the access for the HR Analyst should be undertaken and access removed / disabled where no longer required.	High	Agree – access to be reviewed and removed where no longer required.	Head of HR and Organisational Development	December 2023
9. Consideration should be given to ICT undertaking the System Administration role within iTrent. This would assist with the separation of duties, referred to in recommendation 1.	Medium	Agree – will discuss transfer of responsibilities with IT Manager.	Head of HR and Organisational Development	December 2023
10. The quarterly checks of user access to iTrent should be resumed.	Medium	Agree - checks to be resumed.	HR Analyst	August 2023

TAX – IR35 & P11D – 2022/23



Key Findings

Areas of positive assurance identified during the audit:

- P11D's are produced annually, and notifications are provided to employees.

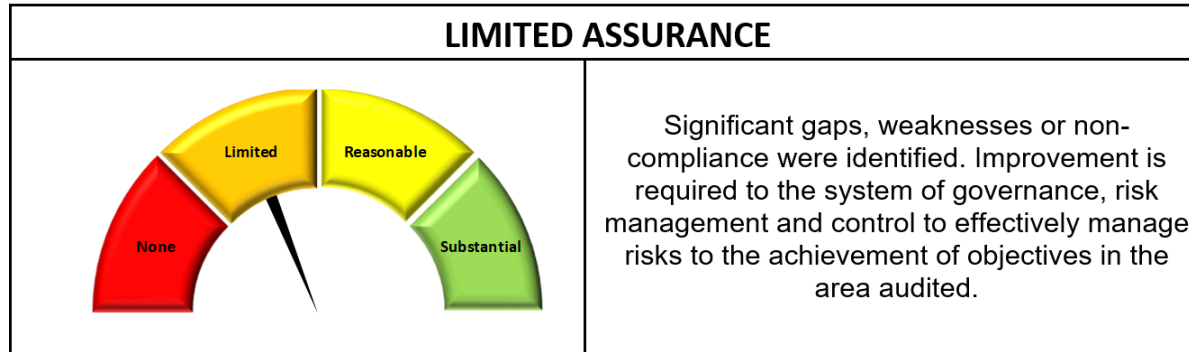
The main areas identified for improvement are:

- Procedure to follow when recruiting consultants / temporary staff.
- Record keeping in relation to the assessment of IR35 status.
- Adherence to Contract Procedure Rules.
- Claiming and recording of VAT on expenses.
- Updating of Long Service and Retirement Award Schemes.

Recommendation	Priority	Response/Agreed Action	Officer Responsible	Implementation Date
1.The guidance for managers to follow when recruiting consultants and agency staff should be further developed and detail the full process to be followed. This should include where relevant documentation should be retained. The guidance should be formally agreed and circulated to managers, with periodic reminders being issued.	High	Agreed – guidance has been produced in connection with staffing approvals and is being presented to CLT.	Finance Team Manager and Head of Human Resources and Organisational Development.	June 2023
2. All IR35 documentation should be held in one central location. This should be detailed in the guidance document, referred to in recommendation 1 above. It is important to consider that should HMRC undertake an inspection this information would need to be easily accessible.	High	As above.	As above.	As above.
3.All managers should be contacted to obtain details regarding consultants or agency staff that are appointed. An up-to-date central record should be retained with full details of the contract period and IR35 assessment and documentation.	High	Agreed. Email to be sent to all managers to request information.	Head of Human Resources and Organisational Development.	June 2023
4. Officers are reminded of the need to ensure that, where agencies or consultants are employed outside of the agency contract, Contract Procedure Rules are relevantly followed, and evidence is retained to support this.	High	Agreed – new CPR's to be issued in May which contains flowchart detailing process to follow when using agency workers. Flowchart to be produced in consultation with Legal Services.	Finance Team Manager.	June 2023.
5.The new supplier form should be updated to include a section to confirm that IR35 status has been assessed, where applicable and information has been sent to the central record.	Low	Agreed. To be included as part of update to reflect new procurement procedures.	Exchequer Services Team Leader.	September 2023.
6.The possibility of using iTrent to record and calculate P11D benefits should be explored.	Medium	iTrent is unable to support P11D but their recommended product – P11D Organiser is used to provide P11D's. Will look at the use of Excel	Finance Team Manager	July 2023

		spreadsheets to see if this process can be streamlined.		
7.The iTrent Employee and Manager Self Service guides should be updated to clearly show how to input and authorise expense claims containing VAT. Additionally, a reminder should be issued to managers informing them of their responsibility when authorising expense claims to ensure that VAT this has been correctly recorded.	High	Agreed	Head of Human Resources and Organisational Development.	August 2023.
8.The possibility of including prompts / guidance pop-ups on iTrent, when inputting expenses, should be explored.	Medium	Agreed – will review the current declaration on iTrent which staff agree to when completing claims and update where required.	Finance Team Manager	September 2023.
9.The Long Service Award and Retirement Award Scheme details should be updated on an annual basis. This should include detailing the correct index used to calculate increases.	Medium	Agreed – CPI will be used to calculate increases.	Head of HR and Organisational Development	August 2023.

CHOICE BASED LETTINGS – 2022/23



Key Findings

Areas of positive assurance identified during the audit:

- There are adequate and up to date documented strategies, policies and procedures in place to cover all aspects of the housing allocation process.
- Weekly advertising cycles have been in place during the period 6 June 2022 to 18 May 2023.
- Initial offers were made promptly following the bidding cycle end.

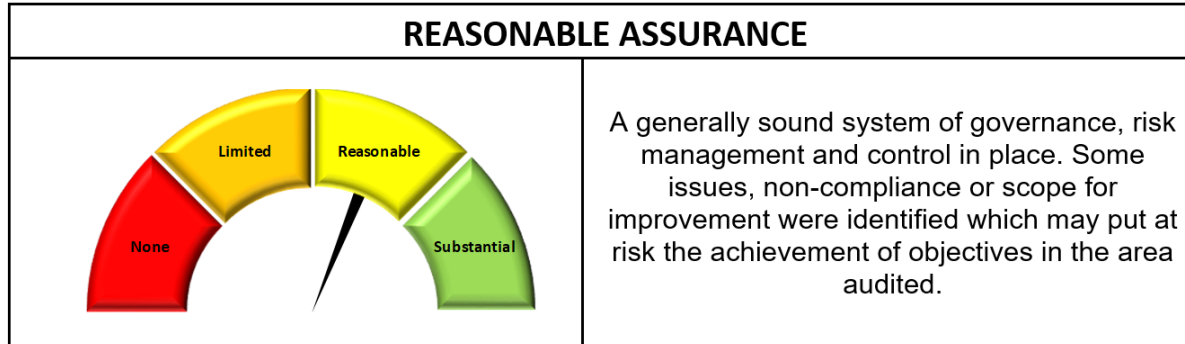
The main areas identified for improvement are:

- Proactive monitoring of the register and regular review of band expiry dates.
- Application statuses require review to establish accurate performance data.
- Regular monitoring of suspended applications, multiple refusals of accommodation and applicants bidding history should be completed, in accordance with policy.
- The status of adverts is reviewed to ensure they are accurate.
- Shortlisting checks for change in circumstances and rent debit should be documented.
- Declarations of Interest should be completed for officers involved in assessment and allocation processes.

Recommendation	Priority	Response/Agreed Action	Officer Responsible	Implementation Date
1. The housing waiting list is proactively monitored, in accordance with the Housing Allocations Policy.	High	Agree with recommendation will be embedded in job roles as part of the recent restructure.	Housing Strategy and Systems Team Manager, and Housing Choices Team Leader.	October 2023
2. A review of all applications within the register is undertaken to confirm that bands are correctly recorded, with band expiry dates being updated accordingly.	High	The system generates a date for all categories but the policy only defines a review of those priority and high bands. Agree with recommendation. Review band expiry date process with the implementation of the new CBL system.	Housing Strategy and Systems Team Manager, Housing Choices Team Leader and the Module Lead for Aareon Implementation Project.	December 2023
3. The application information on QL is reviewed and where appropriate, applications moved to their correct status to ensure that an accurate workflow can be established. 234	Medium	Officers can pick up that an application which requires assessing as a message does come into the workflow, so no assessments would not be missed. However, the system status doesn't always reflect this. This should be resolved with the introduction of the new CBL system.	Housing Strategy and Systems Team Manager, Housing Choices Team Leader and the Module Lead for Aareon Implementation Project.	April 2024
4. Assessing Officers are reminded that the questionnaires within QL need to be completed in full and appropriately updated when new documentation is provided so that the housing need can be recalculated.	Medium	Agree with recommendation. Officers will also be reminded to complete the band reason outside of the questionnaire.	Housing Strategy and Systems Team Manager and Housing Choices Team Leader.	July 2023
5. Procedures are put in place to ensure applicant bids are regularly monitored.	Medium	Agree with recommendation.	Housing Strategy and Systems Team Manager and Housing Choices Team Leader.	October 2023
6. A review of properties advertised as 'not let' is undertaken to ensure the status of the properties are accurately recorded.	Medium	This could be legacy data from the old system and potentially not a field that is used. Agree to review the data and establish what is going on. Senior Officer reviews are completed during one to ones.	Housing Management Team Leader.	July 2023
7. Procedures are put in place to document the way in which shortlisting was completed and reasons why an applicant may have	High	Preferences are added to adverts.	Housing Management Team Leader.	September 2023

been overlooked are clearly documented.		Agree that this needs to be documented better and it needs to be established how this can be done in the system.		
8. Procedures are put in place to evidence that rent arrears and change in circumstances checks are undertaken, in accordance with policy.	Medium	Confident that checks are being done but agree this needs to be documented better.	Housing Management Team Leader.	September 2023
9. Procedures are put in place to monitor applicants who have been suspended.	High	Suspended cases will be reviewed as cases should not remain in this status indefinitely. Procedures will be developed to ensure these are periodically reviewed.	Housing Strategy and Systems Team Manager and Housing Choices Team Leader.	October 2023
10. Officers involved in the allocation process are required to sign a conflict of interest form which highlights potential areas of conflict and includes a declaration that the officer will inform their manager when a potential a conflict of interest could arise.	High	Agreed with recommendation. All existing staff will be asked to sign a declaration of interest form and this will be introduced as part of the induction process for new starters.	Housing Strategy and Systems Team Manager and Housing Management Team Leader.	August 2023
11. A full review of access to the QL Choice Based Lettings system is carried out. This should include the disabling of generic user accounts and ensure user access is appropriate to each user's job role. The review should be carried out on a regular basis going forward.	Medium	A review of housing and choices working groups will be undertaken to ensure levels of access are appropriate to job roles. New starter and leavers access processes have recently been updated. Six monthly reviews of access will be completed going forward, in partnership with ICT.	Income and Systems Team Leader.	July 2023

ANTI-SOCIAL BEHAVIOUR - 2022/23



Key Findings

Areas of positive assurance identified during the audit:

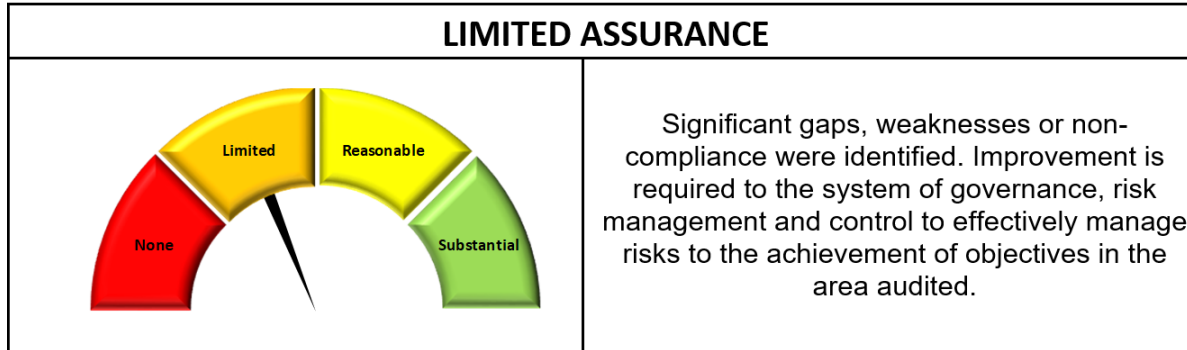
- There are regular meetings at strategic (Safer North West Leicestershire Partnership) and project levels (Project Action Groups).
- There is an update to Community Safety Plan in place.
- All key procedures are documented and are accessible to staff and members of the public.
- There is a sufficient reporting structure in place.
- There are procedures in place for identifying, recording, assessing of risk, monitoring, and reporting of incidents, and that this is in line with the approach of the partnership.

The main areas identified for improvement are:

- The Anti-Social Behaviour Policy needs reviewing.
- Performance indicators are introduced to measure complaints satisfaction and to measure performance against the incremental approach/ASB policy.

Recommendation	Priority	Response/Agreed Action	Officer Responsible	Implementation Date
1. The Anti-social Behaviour Policy is reviewed as stated to ensure it complies with the Anti-Social Behaviour Act 2003, Crime and Disorder Act 1988 and Anti-Social Behaviour, Crime and Policing Act 2014.	Medium	Agreed as per recommendation. This will require multi agency and Community Safety and Environmental Health services input and consultation and will need Cabinet approval. This is reflected in the implementation date.	Housing Management Team Manager.	March 2024
2. The performance indicators are reviewed and where appropriate new indicators added to measure performance against the incremental approach.	Medium	Review the indicators in line with the review of the ASB policy. With the intention to make the indicators for community safety and housing the same.	Housing Management Team Manager.	March 2024
3. Statistical information and benchmarking is completed to ensure comparison for best practice, and identifying trends, in accordance with the ASB Policy.	Medium	This statement within the policy was intended for housing, as the policy is driven by housing legislation and will be reviewed as part of the policy.	Housing Management Team Manager.	March 2024

RENT ACCOUNTING & ARREARS



Key Findings

Areas of positive assurance identified during the audit:

- Annual and new rents are set in line with the Rents Policy and appropriately uploaded to the system.
- Collection rates are regularly monitored for both rental income and arrears.
- Suspense accounts are regularly reviewed, and items promptly investigated and cleared.
- User access to the Housing system is appropriate and procedures are in place to identify and remove access for leavers.

The main areas identified for improvement are:

- Identifying of policies and procedures that require review and update.
- Production of a Corporate Debts Policy covering all council debts.
- Review of the necessity to remove properties from the rent debit.
- Processes to review rent accounts with high credit balances.
- Posting of the rent debit to the general ledger to enable reconciliations between the two systems to be carried out on a regular basis.
- Timely completion and investigation of reconciling items – housing rents to cash receipting reconciliation.
- Investigating mismatches on balances between tenancy enquiry and rent history screens on individual tenancies.

Recommendation	Priority	Response/Agreed Action	Officer Responsible	Implementation Date
1. The policies and procedures held by both the Rent Accounting and Housing Management Teams should be reviewed and updated where necessary. Any obsolete / out of date policies should be archived.	Medium	Agreed – consultation is required for certain policies. This can also be picked up as part of the Policy audit whereby all council policies are listed, with the author and recommended review date.	Housing Strategy and Systems Team Manager and Housing Management Team Manager.	Dec 2023
2. A Corporate Debt Policy should be produced which identifies where responsibility for collection of different types of debt lies and sets out the principles and standards in relation to contact, recovery process, repayments, and benefit / money advice.	High	Agree – a cross department group will be established led by finance to develop the Policy.	Head of Finance and Deputy S151 Officer	June 2024
3. A review as to the circumstances in which properties are taken 'out of debit' and whether this is the correct action to take should be carried out. Where a decision is made to continue to take properties 'out of debit', then the relevant policy / procedure needs to be updated.	High	Agreed, this will be reviewed along with the decision-making process.	Head of Housing	June 2024
4. Consideration should be given to adding performance targets for collection of current and former tenant rent arrears to Team Plans.	Low	This will be included in the business planning process for SMART targets.	Housing Strategy and Systems Team Manager and Housing Management Team Manager.	July 2023
5. A process is introduced to ensure that all former tenant arrears cases are reviewed on a regular basis.	Medium	Agreed this will be reviewed. There will be KPI's brought in for the housing managers to ensure more proactive arrears management.	Housing Strategy and Systems Team Manager and Housing Management Team Manager.	Sept 2023

6. The rent account with a credit balance in excess of £9,000 should be reviewed and contact made with the tenant/s to discuss.	High	Agreed	Head of Housing	Aug 2023
7. Accounts in credit should be regularly reviewed and actioned to ensure that amounts do not become excessive, and amounts are correctly credited back to the original payment account to reduce the risk of fraud and money-laundering.	High	Agreed	Head of Housing	Oct 2023
8. To ensure that action is taken as recommended above the appropriate policy and procedure documents should be updated to incorporate review of rent accounts in credit.	High	Agreed	Head of Housing	Oct 2023
9. Reconciliations should be completed in a timely manner, with any issues being investigated as soon as identified.	High	Agreed	Housing Strategy and Systems Team Manager	July 2023
10. With the introduction of Unit 4 (new Finance System) the rent debit should be uploaded automatically from the Housing System to the General Ledger each week. This should enable weekly reconciliations between the two systems to be carried out.	High	Agreed	Housing Strategy and Systems Team Manager	Aug 23
11. The issue regarding mismatches of balances between the tenancy enquiry screen and rent history screen should be investigated and resolved. Until resolved a regular review should be undertaken to identify any similar mismatches.	High	This issue has now been resolved with alerts in place to identify any future instances. Further work will be followed up by the Head of Housing to ensure that this will be prevented in future.	N/A	Already implemented.

RECOMMENDATIONS TRACKER – EXTENDED RECOMMENDATIONS AS AT 30 JUNE 2023

Audit Year	Audit	Recommendation	Priority	Response/ Agreed Action	Responsible Officer	CLT	Original Due Date	1st Follow up comments	Extension Date
2021/22	Corporate Estates Management	1.A review of all compliance policies and processes is undertaken to establish single corporate policies and comprehensive procedure guides to ensure a consistent approach across the whole of the authority. All policies and procedures should be stored with accessibility for relevant officers.	High	Bearing in mind this groups inception during the pandemic, this group has been operational in nature and considering issues such as contracting and ensuring operational compliance and managing operational risk. As a minimum the following corporate policies will be developed to address this observation (the below are based on risk prioritisation): Legionella Asbestos Fire Risk Management General Health, Safety & Security Electrical Management	Property Services Team Manager (for drafting)	Head of Economic Regeneration	Dec-22	Update - consultants have been employed to develop a Corporate Asset Management Toolkit. This will cover frequency of inspections and recording of compliance.	Jul-23
2021/22	Corporate Estates Management	2 A performance monitoring and reporting framework is introduced which includes contractor and legislative compliance performance monitoring and periodic reporting to the Statutory Duty Group and, where necessary, the Corporate Leadership Team.	High	Overlapping with the audit we have begun the introduction of a performance monitoring framework, utilising a RAG system. This will be reported through to CLT. It would be beneficial to include properties not managed by property services into this report.	Head of Economic Regeneration	Head of Economic Regeneration	Oct-22	Update - consultants have been employed to develop a Corporate Asset Management Toolkit. This will cover frequency of inspections and recording of compliance.	Jul-23
2021/22 241	Corporate Estates Management	3 To ensure that the authority is fully meeting its legislative responsibilities in an efficient and effective manner consideration is given to introducing a true corporate landlord model for corporate property.	High	Since the publication of the 2020 report, there has been considerable change in both the operation of the council, its ability to address some strategic issues due to the pandemic, and more recently changes in property service management, housing senior management and the Chief Executive, along with changes to our accommodation strategy. So as to address the above we will undertake a further assessment of options for the operation and scope of an overall property function spanning all of our assets, and consider how this is best addressed in the future.	Strategic Director	Strategic Director	Mar-23	Extended to align with other recommendations	Jul-23
2021/22	Corporate Estates Management	4 The process for recording and monitoring issues through the compliance tracker is fully implemented and a reporting framework is put in place, to ensure that any remedial actions or works required are identified and tracked to fruition in a timely manner	Medium	Agreed – for the property services managed properties. This may take longer to fully implement if we follow a corporate landlord model. If not then there will not be assurance for all properties.	Head of Economic Regeneration	Head of Economic Regeneration	Oct-22	Update - consultants have been employed to develop a Corporate Asset Management Toolkit. This will cover frequency of inspections and recording of compliance.	Jul-23
2021/22	Corporate Estates Management	5 The review of the Asbestos process is completed and implemented to ensure the council are confident they are complying with regulations.	High	Agreed.	Head of Economic Regeneration	Head of Economic Regeneration	Oct-22	Update - consultants have been employed to develop a Corporate Asset Management Toolkit. This will cover frequency of inspections and recording of compliance.	Jul-23
2021/22	Corporate Estates Management	6 A comprehensive record of all assets and statutory inspections/ checks that are required by the Council is introduced. These records should cover all services and be monitored and reported against on a regular basis to ensure testing/ checks have taken place as required. Note: This recommendation was made in the Health and Safety Audit, undertaken in February 2021 (due for implementation in June 2021) and as yet has not been implemented.	High	Not all of these assets are owned by the authority. The scope of the contracts need to be known and recorded and performance monitored against this. Where assets are owned by the authority these will be detailed as required.	Head of Economic Regeneration	Head of Economic Regeneration	Mar-23	Extended to align with other recommendations	Jul-23

2021/22	Project Management	1. A project management policy is implemented that describes the essential elements of all projects/ programmes (e.g. project / programme identification through to authorisation, officer responsibilities, reporting requirements, requirement of the use of the toolkit etc), to ensure that all projects are effectively managed, and relevant governance and controls are in place.	High	Agreed. CLT need to revisit and agree the programme framework, review/refresh the toolkit, to see if it is still relevant, and then look at the resources for programme management with the new Chief Executive, including looking at where the function sits again, if needed. There is project management support to projects but there is not clear programme management, which is owned and maintained by one person/ service area, and which then collates and reports to CLT/ Members via relevantly timed reports.	Chief Executive, Directors, Monitoring Officer, Section 151 Officer.	CLT	Dec-22	Recommendation extended due to corporate review	Sep-23
2021/22	Project Management	2. A corporate approach to project management is agreed, implemented, relevantly managed, and communicated to all staff on a consistent and regular basis.	High	As above	Chief Executive, Directors, Monitoring Officer, Section 151 Officer.	CLT	Dec-22	Recommendation extended due to corporate review	Sep-23
2021/22	Project Management	3. All corporate projects should be monitored and recorded.	High	As above	Chief Executive, Directors, Monitoring Officer, Section 151 Officer.	CLT	Dec-22	Recommendation extended due to corporate review	Sep-23
2021/22	Project Management	4. The role of the Organisational Performance Team in monitoring of projects, as referred to in the report to CLT, should be pursued.	High	As above	Chief Executive, Directors, Monitoring Officer, Section 151 Officer.	CLT	Dec-22	Recommendation extended due to corporate review	Sep-23
2021/22	Project Management	5. A reporting structure is agreed and disseminated to ensure all relevant parties are aware of projects, progress of projects and any issues and reports are presented in a timely manner.	Medium	As above	Chief Executive, Directors, Monitoring Officer, Section 151 Officer.	CLT	Dec-22	Recommendation extended due to corporate review	Sep-23
2021/22 242	Project Management	6. The highlight reports to boards should contain details of the project approval.	Medium	As above	Chief Executive, Directors, Monitoring Officer, Section 151 Officer.	CLT	Dec-22	Recommendation extended due to corporate review	Sep-23
2021/22	Project Management	7. Following agreement of a corporate approach to Project Management suitable training should be made available to enable staff to effectively manage projects.	High	As above	Chief Executive, Directors, Monitoring Officer, Section 151 Officer.	CLT	Dec-22	Recommendation extended due to corporate review	Sep-23

2023/24 INTERNAL AUDIT PERFORMANCE

Performance Measure	Position as at 30.06.2023	Comments
Achievement of the Internal Audit Plan	0%	Two audits in progress, one audit in planning stage.
Quarterly Progress Reports to Management Team and Audit and Standards Committee	On track	
Follow up testing completed in month agreed in final report	On track	
Annual Opinion Report - July 2023 Audit and Governance Committee Meeting	Achieved	
100% Customer Satisfaction with the Internal Audit Service	100%	Based on two for 2022/23.
Compliance with Public Sector Internal Audit Standards	Conforms	External inspection carried out w/c 30 November 2020 which confirmed that the Council conforms with the Public Sector Internal Audit Standards.

This page is intentionally left blank

NORTH WEST LEICESTERSHIRE DISTRICT COUNCIL

AUDIT AND GOVERNANCE COMMITTEE – WEDNESDAY 26
JULY 2023



Title of Report	INTERNAL AUDIT ANNUAL OPINION REPORT 2022-23	
Presented by	Kerry Beavis Audit Manager	
Background Papers	Public Sector Internal Audit Standards	Public Report: Yes
Purpose of Report	<p>To present the annual internal audit opinion on the overall adequacy and effectiveness of the Council's framework of governance, risk management and internal control.</p> <p>This is required by the Public Sector Internal Audit Standards and should be used to inform the Annual Governance Statement.</p>	
Recommendations	THAT THE COMMITTEE NOTES THIS REPORT AND COMMENTS AS APPROPRIATE.	

Policies and other considerations, as appropriate	
Council Priorities:	An effective internal audit service and risk-based audit plan supports all council priorities.
Safeguarding:	No specific safeguarding considerations identified during our 2022-23 audit work.
Equalities/Diversity:	No specific equalities or diversity considerations identified during our 2022-23 audit work.
Customer Impact:	No specific customer impact however improvements to the overall control environment would potentially benefit all customers.
Economic and Social Impact:	No specific economic and social impact identified during our 2022-23 audit work.
Environment and Climate Change:	No specific environment and climate change impact identified during our 2022-23 audit work.
Consultation/Community Engagement:	The Head of Legal and Support Services, the Interim Director of Resources (S151) and the Chief Executive have been consulted.
Risks:	Not presenting this report to Committee would mean that we have not complied with the Public Sector Internal Audit Standards.
Officer Contact	Kerry Beavis Audit Manager Kerry.beavis@nwleicestershire.gov.uk



INTERNAL AUDIT SHARED SERVICE

North West Leicestershire District Council

Internal Audit Annual Report 2022/23

INTRODUCTION

- 1.1 This is the annual report of the Chief Audit Executive (Audit Manager) as required by the Public Sector Internal Audit Standards (PSIAS). It covers the period 1 April 2022 to 31 March 2023 for North West Leicestershire District Council.
- 1.2 This report includes the Audit Manager's annual opinion on the overall adequacy and effectiveness of the organisation's framework of governance, risk management and control. This is formulated by taking in to account the following –
- All audits completed during the year.
 - Any follow up actions taken in respect of audits from previous periods.
 - High priority recommendations not accepted by management or acted upon and any associated risks.
 - The effect of any significant changes in the Council's objectives, activities or systems.
 - Matters arising from previous reports to the Audit and Governance Committee.
 - Whether any limitations have been placed on the scope of Internal Audit (there have not been any).
 - The extent to which resources constraints may impinge upon the Internal Audit Manager's ability to meet the full audit needs of the Council.
 - What proportion of the Council's audit need has been covered to date.
 - The results of work performed by other assurance providers including the work of the External Auditors.
- 1.3 This report also includes:
- A summary of internal audit work carried out during 2022/23 which supports the opinion.
 - Issues relevant to the preparation of the Annual Governance Statement.
 - Internal Audit's Quality Assurance and Improvement Programme (QAIP).
 - A statement on conformance with the Public Sector Internal Audit Standards.

2. CHIEF AUDIT EXECUTIVE (AUDIT MANAGER) OPINION 2022/23

- 2.1 2022/23 has been a particularly difficult year in terms of resources and staff turnover both within the internal audit section and the areas audited. The audit service has been unable to recruit to a vacant post. However, this has been addressed with the Corporate Leadership team and the audit partners and a new structure has been agreed to ensure that going forward the audit coverage will be proportionate to the Council's need.

Across other areas of the authority audits have had to be cancelled due to staffing levels, this was particularly prevalent in the housing section, this in turn is of concern as controls will be weakened due to this issue. An additional area of concern has been the delay in the implementation of the finance system, leading to internal audit being unable to carry out audits within this area for a second year.

Internal audit has continued to provide the additional support required for assurance on grants, specifically the energy grants.

- 2.2 In line with the Public Sector Internal Audit Standards Internal Audit have worked flexibly throughout the year whilst still ensuring a sufficient, although reduced, level of audit coverage to allow me to give an opinion on the overall adequacy and effectiveness of the framework of governance, risk management and control (the control environment). In giving this opinion it should be noted that assurance cannot be absolute.
- 2.3 For the 12 months ended 31 March 2023, I am only able to give **limited assurance** on the overall control environment. To be consistent with our Internal Audit opinion definitions, this means that significant gaps, weaknesses, or non-compliance were identified. Improvement is required to the system of governance, risk management and control to effectively manage risks to the achievement of objectives in the area audited. As this is not a positive assurance overall it is expected that a corporate management action plan will be put in place to respond to this annual opinion.
- 2.4 My opinion is based on the following:
- All internal audit work undertaken during the year, this includes advisory work as well as assurance, and supports the view on internal control arrangements.
 - Follow up audit work in respect of audit recommendations.
 - My knowledge of the Council's governance and risk management structure and processes.
- 2.5 There have been no impairments to the independence of internal auditors during the year.

3. SUMMARY OF INTERNAL AUDIT WORK DURING 2022/23

- 3.1 The risk based internal audit plan for 2022/23 was presented and approved by the Audit and Governance Committee on 20 April 2022. Progress against this plan has been reported to Audit and Governance Committee throughout the year as part of the quarterly Internal Audit progress reports.
- 3.2 A summary of the audit opinions given in 2022/23 is detailed in Table 1 below. The opinion for individual audits is included in Appendix A for information, along with a comparison of the work delivered against the audit plan.

Table 1

Opinion	Definition	Number
Substantial	A sound system of governance, risk management and control exists, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited	0
Reasonable	There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified which may put at risk the achievement of objectives in the area audited	3
Limited	Significant gaps, weaknesses or non-compliance were identified. Improvement is required to the system of governance, risk management and control to effectively manage risks to the achievement of objectives in the area audited.	5
No Assurance	Immediate action is required to address fundamental gaps, weaknesses or non-compliance identified. The system of governance, risk management and control is inadequate to effectively manage risks to the achievement of objectives in the area audited	-
Total number of audit reports		8

3.3 Three of the Council's key financial systems (Benefits, Business Rates and Council Tax) are provided by the Leicestershire Revenues and Benefits Partnership. For 2022/23 the internal audit service at the Partnership was provided by Mazars. The overall assurance of the 21/22 audit of council tax and business rates, reported to the Leicestershire Partnership Revenues and Benefits Joint Committee during 2023, was reasonable assurance.

3.4 Internal Audit follow up progress against recommendations in line with the timescales agreed at the time of issuing reports. The Corporate Leadership Team are updated on monthly on the progress of the recommendations and Audit and Governance Committee is updated on the Council's progress against the recommendations as part of the quarterly Internal Audit progress reports, as well as giving details of ongoing or overdue recommendations. A summary of the recommendation tracking results for 2022/23 is included at Appendix B.

4. ISSUES RELEVANT TO THE PREPARATION OF THE ANNUAL GOVERNANCE STATEMENT

4.1 The Internal Audit team have issued 5 audit reports with limited assurance during 2022/23. These should be considered when preparing the Annual Governance Statement:

- Rent Accounting & Rent Arrears
The main areas identified for improvement were the completion of reconciliations, management and monitoring of accounts in both arrears and credit, the production of a corporate debt policy and the review of the removal of properties from the rent debit.

- **Tax – IR35 & P60**
The main areas identified for improvement were the processes to follow and the retention of documentation in relation to the recruitment of consultants/ temporary staff, including the adherence to contract procedure rules, and the correct recording of VAT for expenses claimed.

- **Payroll**
The main areas identified for improvement were the segregation of duties between the HR and payroll functions, the review of the establishment, access to the iTrent system and testing of the system when updates/ patches have been applied.

- **Choice Based Lettings**
The main areas identified for improvement included the management and monitoring of the waiting list, including suspended applications, and the documenting of decisions.

There were no audit reports issued without any assurance during 2022/23.

A number of high priority recommendations were made in respect of other audit reviews undertaken, however as they tend to relate to specific systems and/or service areas, I do not consider it necessary to include them in the Annual Governance Statement.

The Section 151 Officer receives all Internal Audit reports issued therefore they are also able to make their own assessment when completing the Annual Governance Statement should they be of a different opinion.

5. QUALITY ASSURANCE AND IMPROVEMENT PROGRAMME (QAIP) FOR INTERNAL AUDIT

- 5.1 The Public Sector Internal Audit Standards (PSIAS) require the QAIP to include internal and external assessments (see Appendix C for more detail).

- 5.2 The internal assessments applicable to 2022/23 include the following:
 - Monthly performance review meetings attended by the Audit Manager and the Head of Legal and Support Services as well as regular meetings with the Head of Finance.
 - Customer satisfaction surveys were sent out to all Team Managers and/or Team Leaders who had an audit in their service area. Only one return was received for 2022/23 which was overall positive feedback.
 - Quarterly progress reports to the Corporate Leadership Team and Audit and Governance Committee which include monitoring of activity and performance.

- 5.3 The PSIAS require external assessments to be conducted at least once every five years. In December 2020 the shared internal audit service had an external quality assessment and the full report was presented to Audit and Standards Committee on 1st February 2021.

- 5.4 It was the assessor's opinion that Internal Audit at Blaby, Charnwood and North West Leicestershire Councils **conforms with the PSIAS**.
- 5.5 In addition to delivering the annual audit plan and opinion, Internal Audit have added value in the following ways:
- Providing advice and support in undertaking elements of the pre and post payment assurance checks for the Covid-19 Grants and Energy Grants.
 - Providing assurance on various other grants during the year – LAD 1b green grant, DEFRA Biodiversity Grant and COMF grant.
 - Providing ad-hoc advice throughout the year to a wide range of services to help ensure that internal controls are maintained or strengthened.
 - The continued delivery of a successful shared service to Blaby District Council and Charnwood Borough Council. This adds value to all Councils as the audit team shares learning, expertise and best practice.

6. CONFORMANCE WITH THE PUBLIC SECTOR INTERNAL AUDIT STANDARDS

- 6.1 The external assessment conducted in December 2020 concluded that there were no significant gaps in compliance.
- 6.2 I can confirm that during 2022/23 the Internal Audit Shared Service conformed to the Public Sector Internal Audit Standards.

RESULTS OF INDIVIDUAL AUDIT ASSIGNMENTS AGAINST THE 2022/23 AUDIT PLAN

Audit Area	Type	Planned Days	Actual Days	Status	Assurance Level	Recommendations				Comments
						C	H	M	L	
Housing Repairs	Audit	10	16	Cancelled						Cancelled due to staffing issues within the housing department and audit being unable to verify the findings gathered to date.
Housing Planned Maintenance	Audit	10	4	Cancelled						Cancelled due to staffing issues within the housing department and audit being unable to verify the findings gathered to date.
Choice Based Lettings	Audit	8	11.5	Completed	Limited	-	5	6	-	
Rent Arrears	Audit	7	7	Completed	Limited					Included within Rent Accounting audit.
Right to Buy	Audit	8	9.5	Completed	Reasonable	-	4	5	2	
Anti-social behaviour	Audit	8	7.5	Completed	Reasonable	-	-	3	-	
Key financial systems	Risk based	26		Q2/3/4						Deferred until 23/24 due to the delay in the implementation of the new finance system.
Tax	Audit	10	9.5	Completed	Limited	-	5	3	1	
Covid-19 Related Assurance	As required	10	6	As required						
LAD 1b Green Grant	Certification	-	5.5	Completed		-	-	-	-	Addition to plan
Tenant Association Accounts	Advisory and review		2	Completed						Addition to plan
COMF grant funding	Certification		1.5	Completed	N/A	-	-	-	-	Addition to plan
DFG	Certification	1	1	Completed	N/A	-	-	-	-	
Procurement	Audit	10	5	Completed		-	-	-	-	Addition to plan
Rent Accounting	Audit	4	10	Draft	Limited	-	8	2	1	
Payroll	Audit	4	7	Completed	Limited	-	7	3	-	
IT Health Check	Audit			Completed	Reasonable	-	3	4	-	

Recommendations key – see Appendix B

SUMMARY OF INTERNAL AUDIT RECOMMENDATIONS FOLLOW UP 2022/23

Internal Audit follow up progress against critical, high, and medium priority recommendations in line with the timescales agreed at the time of issuing reports. The progress of recommendations is reported to the Corporate Leadership Team on a monthly basis and any overdue recommendations are highlighted to Audit Committee.

The table below shows the progress against recommendations made by Internal Audit during 2022/23. The reason that there is such a high number of recommendations in progress or not yet due is due to the timings of the audit and the agreed implementation dates not then being until 2023/24, these will continue to be reported to Audit Committee.

Recommendation Priority	Recommendations Made	Recommendations Implemented	Recommendations Outstanding (In Progress or Not Yet Due)	Recommendations Overdue
Critical	-	-	-	-
High	32	7	25	-
Medium	26	6	20	-
Total	58	13	45	-

Level	Definition
Critical	Recommendations which are of a very serious nature and could have a critical impact on the Council, for example to address a breach in law or regulation that could result in material fines/consequences.
High	Recommendations which are fundamental to the system and require urgent attention to avoid exposure to significant risks.
Medium	Recommendations which, although not fundamental to the system, provide scope for improvements to be made.
Low/Advisory	Recommendations concerning issues which are considered to be of a minor nature, but which nevertheless need to be addressed. Issues concerning potential opportunities for management to improve the operational efficiency and/or effectiveness of the system.

QUALITY ASSURANCE AND IMPROVEMENT PROGRAMME 2022-23

Activity	PSIAS	Result/comments	Frequency
External Quality Assessment	1310	December 2020 Assessment - no significant gaps in compliance.	Every 5 years.
Annual Declaration of Interests	1130	Forms completed in April 2022, this includes Code of Ethics and Principles.	Annual
Customer satisfaction surveys	1311	One received for 2022/23. Positive overall.	After each audit
Performance indicators reported in progress reports	1311	Performance indicators included in all quarterly reports to corporate leadership team and Audit Committees.	Quarterly
Improvement actions/continuous improvement	1311	An internal action plan produced for 2022/23 detailing improvement actions which included rolling review of the internal audit service to ensure compliance with standards.	Ongoing
Review of all audit engagements and reports	1311, 2340	All audit engagements and reports are reviewed by the audit manager to ensure compliance with PSIAS in terms of meeting audit objectives and quality.	Every audit
Monthly performance reporting and meetings	1311	Monthly performance meetings with Head of Legal and Support Services (Monitoring Officer) and the Head of Finance (S151 Officer).	Monthly
Annual review of internal audit charter	1000	Shared Service Charter updated with only minor amendments and reported to Audit & Governance Committee in October 2022. Annual review takes place in September each year.	Annual
Performance and development review process for staff and training and development records.	1200	All review meetings with team have taken place and the training and development recorded within system for all training and development identified and completed. Officers recording their CPD in line with their professional body requirements do not need to duplicate records.	Bi- annual review meetings

This page is intentionally left blank

NORTH WEST LEICESTERSHIRE DISTRICT COUNCIL

AUDIT AND GOVERNANCE COMMITTEE – WEDNESDAY, 26
JULY 2023

Title of Report	MANAGEMENT RESPONSE TO INTERNAL AUDIT OPINION 2022/23	
Presented by	Glenn Hammons Interim Director of Resouces	
Background Papers	Internal Audit Annual Report – Audit & Governance Committee – 26 July 2023	Public Report: Yes
Purpose of Report	The report provides a management response and action plan to address the findings of the Annual Internal Audit Opinion 2022/23.	
Recommendations	THE COMMITTEE ARE RECOMMENDED TO: 1. APPROVE THE ACTION PLAN SET OUT IN APPENDIX 1 WHICH ADDRESS THE FINDINGS OF THE INTERNAL AUDIT OPINION 2022/23. 2. AGREE PROGRESS UPDATES TO BE REPORTED AT FUTURE MEETING OF THE AUDIT AND GOVERNANCE COMMITTEE.	

1.0 BACKGROUND

- 1.1 In accordance with the Public Sector Internal Audit Standards (PSIAS) the Chief Audit Executive (the Internal Audit Manager at North West Leicestershire District Council) is required to produce an annual report. The report covering the financial year 2022/23 is set out on a separate item on the Committee's agenda.
- 1.2 The Opinion covers the overall adequacy and effectiveness of the organisation's framework of governance, risk management and control. The draft Internal Audit Annual Opinion for 2022/23 is 'Limited Assurance'.
- 1.3 It is recognised by the Council this level of assurance is not acceptable and requires improvements to be made.
- 1.4 In response to the Opinion the Council have instigated and established an Action Plan to address the concerns and issues raised.

2.0 MANAGEMENT RESPONSE AND ACTION PLAN

- 2.1 The assurance provided by the internal audit function is an important part of the overall corporate governance framework of the Council. The Council are committed to improving the effectiveness of internal audit to optimise assurance. It is recognised this will require process, procedural and, most importantly, cultural change across the Council to provide the appropriate level of assurance.
- 2.2 In response to the Opinion, and recognising the context within which the Opinion has been determined, the Council have developed an Action Plan. The Action Plan is set out at Appendix 1 of the report.
- 2.3 It is important the Action Plan is implemented. To ensure there is a clear focus on delivery of the Action Plan within the Council a clear governance and reporting process is required. From a management perspective the progress against delivery of the Action Plan will be reported to the Statutory Officer Group at its meetings. A status update report on delivery against the Action Plan will be provided to Audit and Governance Committee at future meetings.

Policies and other considerations, as appropriate	
Council Priorities:	<ul style="list-style-type: none"> - Supporting Coalville to be a more vibrant, family-friendly town - Support for businesses and helping people into local jobs - Developing a clean and green district - Local people live in high quality, affordable homes - Our communities are safe, healthy and connected
Policy Considerations:	Not applicable.
Safeguarding:	Not applicable.
Equalities/Diversity:	Not applicable.
Customer Impact:	Not applicable.
Economic and Social Impact:	Not applicable.
Environment and Climate Change:	Not applicable.
Consultation/Community Engagement:	In developing the Action Plan there has been extensive engagement with statutory officers, the Corporate Leadership Team and the Internal Audit Manger.
Risks:	<p>The Council's governance arrangements are a critical part of its operations to ensure decision making is robust and effective.</p> <p>Internal audit is an important part of these governance arrangements.</p> <p>There are a number of risks to the Council if it does not have a properly functioning internal audit function. These potential risks include reputation, poor decision making, fraud, lack of control and inadequate assurance.</p>
Officer Contact	Glenn Hammons Interim Director of Resources glenn.hammons@nwleicestershire.gov.uk

This page is intentionally left blank

Management Actions In Response To Annual Internal Audit Opinion 2022/23

Action	Current Status Position	Work to Fully Implement Action	Timeline for Delivery	Lead Officer	Comments
Deliver the internal audit plan for each year	The Internal Audit Plan for 2023/24 has been signed off by Corporate Leadership Team and approved at Audit & Governance Committee on 26th April 2023	Progress on delivery of the Plan is reported to CLT and A&G Committee throughout year	March 2024	Internal Audit Manager	
		Internal Annual Report for 2023/24 to provide final performance	July 2024		
		Internal Audit team is resourced to deliver the Plan. Position to be reported in Quarterly Report to Audit Governance Committee (see action below)	July 2024		
Strengthen performance management process for implementation of internal audit recommendations	Initial conversations between Statutory Officers and Internal Audit Manager have established initial improvements	Fully review current IA Recs implementation performance management process	Sept 2023	Director of Resources	
		Assign audit recommendations to the officer responsible for implementing them	July 2023	Internal Audit Manager	
		Internal Audit to attend Team meetings at least 6 monthly. [Head of Service to invite Internal Audit. Internal Audit to produce record of meeting]	Sept 2023	Head of Service / Team Manager	
		Enhanced initial process - statutory officer sessions for recommendation owners to justify their plan for delivery of recommendations	July 2023	Director of Resources	Initial meeting planned for 24 July 2023
		Attendance at Audit and Governance Committee for CLT Lead to report progress on delivery. On an exception	Sept 2023	Director of Resources	

Action	Current Status Position	Work to Fully Implement Action	Timeline for Delivery	Lead Officer	Comments
		basis for late or extended recommendations			
Strengthen reporting process to Audit & Governance for internal audit recommendations		Review the reporting process	Sept 2023	Director of Resources	CLT were advised of the enhanced process in June. First Statutory Officers meeting planned for 24 July 2023
		Implement enhanced exception reporting (with focus on extensions and missed deadlines) for recommendation owners with Statutory Officer and at Audit & Governance Committee	December 2023		
		Embed the new process into the Council's way of working	March 2024		
Increased capacity of internal audit resources / team	<ul style="list-style-type: none"> o A review of the team was undertake in Autumn of 2022. o A new structure was agreed by all partner Council's o NWL agreed additional resources as part of its 2023/24 base budget in February 2023. o Recruitment to the new structure has commenced with the successful appointment of an Apprentice role 	Fully recruit to new Internal Audit structure. Currently there are two posts in the process of recruitment.	Sept 2023	Internal Audit Manager	Interim resource is being considered to deliver the Plan if permanent resources are not recruited in a timely manner.
Strengthening senior management structure	The Chief Executive reviewed the senior leadership capacity in the organisation in Autumn 2022. Council approved the structure in February 2023 including a	n/a	n/a	n/a	Complete

Action	Current Status Position	Work to Fully Implement Action	Timeline for Delivery	Lead Officer	Comments
	Director of Resources (s151 officer) and Head of Finance. The Head of Finance role was recruited to in May 2023. The Director has been recruited to and is due to start in September 2023. An interim Director is currently covering the role.				
Improve synergies and linkages between internal and external audit		Internal Audit to have regular meetings with External Audit	October 2023	Internal Audit Manager	
Raise the profile and importance of internal audit in the Council	<ul style="list-style-type: none"> ○ It has been recognised at a senior management level a cultural shift is required within the organisation as internal audit is important to ensure the council performs effectively. ○ The senior leadership team has been strengthened. ○ Additional capacity has been secured for the Internal Audit team. ○ Reference to role of Internal Audit was included in CLT blog in June 2023. 	Communicate the importance of internal audit to staff as part of the overall governance framework of the Council by including an Internal Audit module in corporate governance training.	December 2023	Head of Legal and Support Services	
		Review Internal Audit training on their function/role on Skillgate	March 2024	Internal Audit Manager	
		Directors to ensure their Teams have regard to the assurance framework in their services. Engage internal audit as part of Council Delivery Plan/Business Planning process	December 2023	Directors	
		Internal Audit seen as part of the decision making/grant bids/project set up process	March 2024	Directors and Heads of Service	
		Review project management templates, toolkit and guidance to include input from/ engagement with Internal Audit	March 2024	Director of Resources	

Action	Current Status Position	Work to Fully Implement Action	Timeline for Delivery	Lead Officer	Comments
		Business/Service Plan process and associated templates to be updated to include Internal Audit Plan as a consideration (as part of wider support service engagement)	December 2023	Head of HR & OD	
		Engage internal audit as part of Business/Service Plan process	March 2024	Directors/Heads of Service	
		Consider if Managers Job Description need to be updated to reflect importance of assurance.	March 2024	Head of HR & OD	
		Consider if the staff appraisal process could assist in managing implementation of internal audit recommendations.	September 2023	Head of HR & OD	
		Internal Audit to produce regular blogs, including case studies of usefulness of early/proactive engagement	March 2024	Internal Audit Manager	
Improve the accessibility of internal audit reports on the Council's systems	The Internal Audit team have an existing presence on the Council's intranet	Review the current intranet presence and accessibility for Internal Audit	July 2023	Internal Audit Manager	
		Implement the findings of the review	December 2023		
Implementation of the Council's new finance system to enhance financial control environment	The new finance system was implemented and went live from 1 April 2023. This will improve financial assurance from an internal audit perspective.	n/a	n/a	n/a	Complete.
Meetings between Internal Audit Manager and the Chair of the Audit Committee		Set up regular meetings	July 2023	Internal Audit Manager	

Action	Current Status Position	Work to Fully Implement Action	Timeline for Delivery	Lead Officer	Comments
Compliance with CIPFA Position Statement to ensure the Audit and Governance Committee have the required skills and knowledge	<ul style="list-style-type: none"> ○ Audit and Governance Committee consider in April 2023 	Developing the training plan by working group	Oct 2023	Director of Resources	
	<ul style="list-style-type: none"> ○ Member Working Party established and had their first meeting. 	Delivery of the training plan	On-going		
	<ul style="list-style-type: none"> ○ Training sessions for Members took place on Role of Audit Committee (5 June) and Treasury Management Training (6 July) 	Appointment of independent persons on the Audit & Governance	Oct 2023		

This page is intentionally left blank

NORTH WEST LEICESTERSHIRE DISTRICT COUNCIL

AUDIT AND GOVERNANCE COMMITTEE – WEDNESDAY, 26
JULY 2023

Title of Report	STANDARDS AND ETHICS REPORT - QUARTER 1	
Presented by	Elizabeth Warhurst Head of Legal and Support Services and Monitoring Officer	
Background Papers	None	Public Report: Yes
Purpose of Report	To receive the figures for local determination of complaints and the ethical indicators for Quarter 1 of 2023/2024	
Recommendations	THE REPORT BE RECEIVED AND NOTED.	

1.0 BACKGROUND

1.1 The Standards and Ethics Report provides information in two categories: Local Determination of Complaints and Ethical Indicators.

2.0 CHANGES

2.1 Within the section 'Local Determination of Complaints', paragraph 2.2 has been updated to reference the Local Government Association guidance instead of the Standards for England guidance, which was previously referenced, as the Standards for England no longer exists. Also the timeframe for the Council in determining a response has been reduced from 20 days to 15 days to reflect the 'Council's arrangements for dealing with complaints' as adopted by Full Council last February along with the new Code of Conduct.

2.2 Within the section 'Ethical Indicators' the Use of RIPA powers (Regulation of Investigatory Powers Act 2000) has been added to the table. This had previously been included but in recent iterations of the quarterly report it had been omitted. Following our 3 yearly RIPA inspection it was felt best practise to re-introduce this data.

Policies and other considerations, as appropriate	
Council Priorities:	Our communities are safe, healthy and connected
Policy Considerations:	N/A
Safeguarding:	Safeguarding in relation to Modern Slavery
Equalities/Diversity:	N/A
Customer Impact:	N/A
Economic and Social Impact:	N/A

Environment and Climate Change:	N/A
Consultation/Community/Tenant Engagement:	Customers have the opportunity to report on measures that are included in this report
Risks:	By receiving this information members will be able to manage risks
Officer Contact	Elizabeth Warhurst Head of Legal and Support Services elizabeth.warhurst@nwleicestershire.gov.uk

Standards and Ethics

Quarter 1 Report

2023-2024

Contents

Page 1 - Introduction

Page 2 - Local Determinations of Complaints

Page 3 - Ethical Indicators

Page 4 - Freedom of Information Requests

Page 5 - Definitions

270

Introduction

This is the quarterly report to the Audit & Governance Committee detailing both the figures for the Ethical Indicators and the figures for the Local Determination of Complaints process for 2023/2024.

For clarification purposes the months covered by the quarters are as follows:

Quarter 1 - 1 April to 30 June

Quarter 2 - 1 July to 30 September

Quarter 3 - 1 October to 31 December

Quarter 4 - 1 January to 31 March

The report is split into 2 parts for ease of reference; Part 1 refers to the local determination of complaints, part 2 is the table showing the ethical indicators figures.

The report will enable the Audit & Governance Committee to build up a picture over time of how many complaints are received and where these are coming from. The parts of the Code of Conduct which have been breached will also be recorded to enable training to be targeted effectively.

Local Determination of Complaints

The Monitoring Officer received 3 complaints in Quarter 1 of 2023/24 (1 April 2023 – 30 June 2024).

1 complaint received was unable to be progressed as it was determined that the Councillor was acting in a private capacity.

2.1 Assessment Sub-committee Decisions

There has been 0 Assessment Sub-committee meetings in this quarter.

The Monitoring Officer pursues an informal dispute resolution process prior to initiating formal proceedings via the Sub-committee route.

1 complaint has been resolved informally in Quarter 1. 1 complaint received In Quarter 1 was still ongoing at the end of the quarter.

2.2 Timeliness of Decision

The Local Government Association [guidance](#) states that where the decision has been delegated to an officer the authority should aim to complete their initial assessment of an allegation within 15 working days of receiving a complaint. Where the assessment is sent to a committee, the committee should be set up along similar timescales. The Council has taken this standard and included it in the Council's arrangements for dealing with complaints to aim to hold an Assessment Sub-committee within 15 working days of notifying the parties that informal resolution is not possible

2.3 Review Requests

There have been 0 review requests in Quarter 1. Review requests can only be made following a decision of 'No further Action' by the Assessment Sub-committee where there is submission of new evidence or information by the complainant.

2.4 Subsequent Referrals

None to report – see above

2.5 Outcome of Investigations

None to report – see above

2.6 Parts of the Code Breached

This section is intended to show where there are patterns forming to enable the Audit and Governance Committee to determine where there needs to be further training for Councillors. Targeting training in this way makes it more sustainable and, hopefully, more effective.

So far this year, the following areas of the code were found to have been breached:

N/A

Complaints made to the Monitoring Officer under the Code of Conduct during Q1 2023/24

273

<u>Qtr 1</u> <u>23/24</u>	<u>Complaint from</u>	<u>About district/ parish councillor</u>	<u>Regarding</u>	<u>status</u>
	Member of the public	Parish Cllr	Comments on social media	It was concluded this complaint was unable to be progressed as the subject member was not acting in their capacity as a Councillor at the time
	Member of the public	District Cllr	Comments on social media	Resolved informally
	Member of the public	Parish Cllr	Comments on social media	Ongoing

Ethical Indicators

PERFORMANCE INDICATOR	Q1			Q2			Q3			Q4		
	21/22	22/23	23/24	21/22	22/23	23/24	21/22	22/23	23/24	21/22	22/23	23/24
Instances of concerns raised re Modern Slavery	0	0	0	0	0		0	0		1	0	
Instances of concerns raised re Modern Slavery referred to national agencies	0	0	0	0	0		0	0		0	0	
Number of whistle blowing incidents reported	0	0	0	0	0		0	0		0	0	
Number of Challenges to procurements	0	0	0	0	0		0	0		0	0	
Public interest Reports	0	0	0	0	0		0	0		0	0	
Objections to the Councils Accounts	0	0	0	0	0		0	0		0	0	
Disciplinary action relating to breaches of the Member/Officer Protocol	0	0	0	0	0		0	0		0	0	
Follow up action relating to breaches of the Member/Officer Protocol	0	0	0	0	0		0	0		0	0	
Use of RIPA powers	0	0	0	0	0		0	0		0	0	

Freedom of Information Requests

	Q1			Q2			Q3			Q4		
	21/22	22/23	23/24	21/22	22/23	23/24	21/22	22/23	23/24	21/22	22/23	23/24
Total Number (FOIs)	102	147	157	107	122		90	108		94	196	
% answered on time	82.9%	51%	93%	71.9%	79%		95.1%	60%		86%	78.17%	
Average per month	34	49	52	36	41		30	38		31	65	
Average response time (days)	14	7	11	13	9		10	14		11	15	
Withheld due to exemption/fees (FOI and BAU)*	19	0	13	12	0		15	7		10	13	
Transfers (TFRs)	18	29	18	12	21		24	18		23	28	
Subject access requests (SARs)	1	3	11	2	6		5	5		5	13	
Internal Reviews	0	1	1	2	3		1	3		0	2	
Environmental Information Requests/ Land Charges Searches (personal)	6	4	6	491	4		336	7		11	1	

- This quarter has seen a slight increase in the number of FOI requests.
- The aim is to achieve 90% + response rate. This target has been achieved in Q1.
- The item BAU has been removed from the table. This is because we do not log requests as a BAU on the new system. All requests are logged on the case management system as an FOI/EIR/DP request.

FOI Exemptions for Q1 23/24

276

Exemption	Description	FOI	BAU	Total
S21	Information Already Reasonably Accessible	2		
S22	Information Intended for Future Publication	4		
S27	International Relations			
S28	Relations within the UK			
S29	The Economy			
S30	Investigations			
S31	Law Enforcement	3		
S32	Court Records			
S36	Effective Conduct of Public Affairs			
S38	Endangering Health and Safety			
S39	Environmental Information			
S40	Personal Information of the Requester/Personal Information	1		
S41	Confidentiality			
S42	Legal Professional Privilege			
S43	Trade Secrets and Prejudice to Commercial Interests			
S44	Prohibitions on Disclosure		3	
Total	<i>Number need not match the number of cases. Multiple exemptions may apply to one case.</i>	10	3	0

Definitions

Business as usual Information requested can be sent quickly and easily within the normal course of business

Land Charges specific information about a particular property

Ombudsman Complaint a customer has followed Stage 1 and 2 complaints procedure but unhappy with the outcome they are entitled to take complaint to the Local government Ombudsman who will decide if the Council has a case to answer.

Subject Access Request a request by an individual to see information an organisation holds on them

Transfers requests received that fall out of our remit i.e. Adult social Care or Highways

Environmental Information Request a right for any person to request access to environmental information held by public authorities.

This page is intentionally left blank