



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, 7 August 2024
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 24 April 2024	3 - 6
4. COMMITTEE WORK PLAN	
To note the Committee's work plan	7 - 8
5. ANNUAL AUDIT OPINION	
The report of the Audit Manager	9 - 20
6. MANAGEMENT RESPONSE TO ANNUAL INTERNAL AUDIT OPINION 2023/24	
The report of the Strategic Director of Resources	21 - 44
7. INTERNAL AUDIT PROGRESS REPORT	
The report of the Audit Manager	45 - 82
8. REVIEW OF CORPORATE GOVERNANCE POLICIES	
The report of the Strategic Director of Resources	83 - 222

Circulation:

Councillor P Moulton (Chair)
Councillor D Everitt (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 Abbey Room, Stenson House, London Road, Coalville, LE67 3FN on WEDNESDAY, 24 APRIL 2024

Present: Councillor D Everitt (Chair)

Councillors P Moulton, D Cooper, G Rogers, J G Simmons, R Sutton and A Barker

Officers: Ms K Beavis, Ms K Hiller, Miss E Warhurst, Mr T Devonshire, Mr P Stone, Mr S Outama and Mrs D Harris

External Audit: Mr M Surridge

33. APOLOGIES FOR ABSENCE

Apologies were received from Councillor N Smith and R Boam.

34. DECLARATION OF INTERESTS

There were no interests declared.

35. MINUTES

Consideration was given to the minutes of the meeting held on 24 January 2024.

It was moved by Councillor R Sutton, seconded by Councillor J Simmons, and

RESOLVED THAT:

The minutes of the meeting held on 24 January 2024 be confirmed as an accurate record of proceedings.

36. COMMITTEE WORK PLAN

Consideration was given to the inclusion of any items on the work programme.

37. EXTERNAL AUDIT UPDATE

The Strategic Director of Resources presented the report, in conjunction with a representative from Mazars.

A Member suggested that to call the delay in the auditing of the accounts solely a national issue was to decontextualise and perhaps to obfuscate. The Council was, he said, one of a very small number of local authorities which appeared to have no draft accounts to audit for 2021/22 and 2022/23, putting aside the national problems in the audit industry. Furthermore, many of the Councils in the same position were ones which had attained national infamy due to financial problems in recent years.

The Strategic Director of Resources declined to comment on the position of other local authorities. With regards to NWLDC he informed Members that the 2020/21 statement of accounts had experienced delays, particularly in relation to property, plant, and equipment. This had significantly affected the completion of the outstanding accounts for 2021/22 and 2022/23. Additionally, the finance team had faced capacity issues. Moreover, resources also had to be used towards other financial priorities, such as budget setting.

In response to the member reiterating his concern, the Strategic Director responded that the Council was committed to publishing the accounts and presenting them to the Audit and Governance Committee.

The representative from Mazars said that the External Audits would provide a value for money opinion on the delayed accounts by 31 October 2024. He expected to produce a disclaimer opinion, which expressed confidence on aspects where it could and then considered the value of the information they had as a totality. The Director added that a disclaimer opinion did not necessarily indicate significant financial reporting or financial management issues.

The Member was concerned that this would have a reputational impact. The representative from Mazars accepted that the situation was not ideal, but advised that the Council was not an outlier, and local authorities were relatively safeguarded against reputational damage in this area compared to, say, a corporation.

A Member asked whether draft unaudited accounts were typically published. The Strategic Director of Resources noted that prior to the Coronavirus period the Council had a very good track record of publishing accounts on time and audited, and that the organisation strived to adhere to the CIPFA code. He would write to the Chair and the rest of the Committee to clarify the regulations around publishing draft unaudited accounts, as well as providing further detail in respect of the reasons for the delays.

It was moved by Councillor J Simmons, seconded by Councillor A Barker, and

RESOLVED THAT:

The report be noted.

38. SIRO (SENIOR INFORMATION RISK OFFICER) ANNUAL REPORT

The Head of Legal and Support Services and Monitoring Officer presented the report, with assistance from the ICT Team Manager and the Legal Team Manager.

A Member welcomed the report and praised the work done.

By affirmation of the meeting it was

RESOLVED THAT:

The report be noted.

39. AUDIT AND GOVERNANCE COMMITTEE ANNUAL REPORT 2023/24

The Strategic Director of Resources presented the report.

The Deputy Chair thanked Officers for supporting the Committee through their first year as Members of the Audit and Governance Committee, and other Members concurred.

Councillor R Sutton said that he would be abstaining, due to the issues with the external audit, and requested that it be recorded in the minutes.

It was moved by Councillor G Rogers, seconded by Councillor J Simmons, and

RESOLVED THAT:

The draft report be approved prior to submission to Council on 18 June 2024.

40. DRAFT MEMBER CODE OF CONDUCT ANNUAL REPORT

The Head of Legal and Support Services and Monitoring Officer presented the report.

It was moved by Councillor A Barker, seconded by Councillor P Moulton, and

RESOLVED THAT:

1. The draft Member Code of Conduct Annual Report 2023/24 be noted.
2. Authority be delegated to the Head of Legal and Support Services and Monitoring Officer to make any minor amendments to the report following comments from the Audit and Governance Committee.
3. Council be recommended to endorse the Member Conduct Annual Report 2023/24.

41. INTERNAL AUDIT PLAN 2024-25

The Audit Manager presented the report.

A Member asked whether the Audit Manager was content with the support she was receiving and the capacity of her Team, and in response she said that the Team was now fully recruited to, although this did include an Officer on maternity leave, but her Audit Plan accounted for this, and she was confident moving forwards.

Members then discussed the auditing of Key Financial Systems. The Audit Manager advised that they were always part of the Audit Plan and set out exactly how this had operated in recent years. She said that she would write a note for the Committee to clarify this in greater detail.

It was moved by Councillor R Sutton, seconded by Councillor P Moulton, and

RESOLVED THAT:

1. The report be noted,
2. The 2024/25 Internal Audit Plan be approved.

42. ANNUAL GOVERNANCE STATEMENT 2021/22 AND 2022/23

The Strategic Director of Resources presented the report.

It was moved by Councillor A Barker, seconded by Councillor J Simmons, and

RESOLVED THAT:

The report be approved.

43. INTERNAL AUDIT PROGRESS REPORT

The Audit Manager presented the report.

A Member felt that where progress against the plan had not been made it should be more clearly highlighted.

It was moved by Councillor R Sutton, seconded by Councillor P Moulton, and

RESOLVED THAT:

The report be noted.

44. CORPORATE RISK UPDATE

The Strategic Director of Resources presented the report.

A Member asked whether staff were continuing to leave the organisation in significant numbers and whether this contributed to the increased risk.

The Strategic Director of Resources advised that the Council was operating in a challenging national context, but staffing was something which the Corporate Leadership Team recognised as a key priority. He would also consider how best to feed in these other ongoing discussions about staffing, by the Corporate Leadership Team and at other Committees, into future Risk Workshops.

It was moved by Councillor J Simmons seconded by Councillor A Barker, and

RESOLVED THAT:

The report be noted.

45. QUARTER 3 TREASURY MANAGEMENT ACTIVITY REPORT

The Strategic Director of Resources presented the report.

A Member was pleased to see the good financial performance reported.

A Member asked about the loan of £5 million to Birmingham City Council and whether it had been impacted by the S114 Notice which Birmingham City Council had issued in Autumn 2023. In response, the Strategic Director of Resources advised that since the end of Quarter 3, this loan had been paid off without delay and there were no further outstanding loans with Birmingham City Council.

It was moved by Councillor R Sutton, seconded by Councillor J Simmons, and

RESOLVED THAT:

1. The Treasury Management 2023-24 Quarter 3 Activity Report (Appendix A) be noted.
2. The Prudential Indicators 2023-24 Quarter 3 Update (Appendix B) be noted.

46. STANDARDS AND ETHICS REPORT - QUARTER 4

The Head of Legal and Support Services and Monitoring Officer presented the report.

It was moved by Councillor R Sutton, seconded by Councillor G Rogers, and

RESOLVED THAT:

The report be noted.

The meeting commenced at 6.30 pm

The Chairman closed the meeting at 7.47 pm

AUDIT AND GOVERNANCE COMMITTEE – WORK PROGRAMME (as at 30/07/24)

Issue	Report Author	Meeting at which will be reported
22 August (tbc)		
Standards and Ethics Report - Quarter 1	Charlotte Smith, Apprentice Solicitor	22 August 2024
Corporate Risk Update To provide Committee members with an update in respect of the Council's corporate risk register.	Paul Stone, Strategic Director of Resources (Section 151 Officer)	22 August 2024
Local Government and Social Care Ombudsman Annual Review Letter 2023/24	Elizabeth Warhurst, Head of Legal and Support Services (Monitoring Officer)	22 August 2024
Treasury Management Stewardship report 2023/24	Anna Crouch, Head of Finance	22 August 2024
Internal Audit Progress Continuation Report	Kerry Beavis, Audit Manager	22 August 2024
September 2024		
Statement of Accounts 2021/22 To members to approve the Statement of Accounts 2021/22.	Anna Crouch, Head of Finance	25 September 2024
Draft Accounting Policies 2023/24	Anna Crouch, Head of Finance	25 September 2024
Review of the Council's Arrangements for Dealing with Complaints about Councillors	Kate Hiller, Legal Team Manager and Deputy Monitoring Officer	25 September 2024
November 2024		
Annual Review of the Council's Constitution	Kate Hiller, Legal Team Manager and Deputy Monitoring Officer	20 November 2024
Annual Governance Statement 2023-24 Approval of the Annual Governance Statement for 2023-24	Paul Stone, Strategic Director of Resources (Section 151 Officer)	20 November 2024
Standards and Ethics Report - Quarter 2	Charlotte Smith, Apprentice	20 November 2024

Issue	Details	Report Author	Meeting at which will be reported
	Solicitor		Treasury Management Update Report - Quarter 2 To present the quarterly treasury management report to members,
Annual Governance Statement 2023/24 The Council is required to produce an Annual Governance Statement which is presented as part of its annual Statement of Accounts.	Anna Crouch, Head of Finance	20 November 2024	February 2025
Standards and Ethics Report - Quarter 3	Paul Stone, Strategic Director of Resources (Section 151 Officer)	20 November 2024	Treasury Management Update Report - Quarter 3 To present the quarterly treasury management report to members.
Standards and Ethics Report - Quarter 3	Charlotte Smith, Apprentice Solicitor	5 February 2025	March 2025
There is currently nothing scheduled for this meeting			
April 2025			
Annual Member Conduct Report	Charlotte Smith, Apprentice Solicitor	23 April 2025	June 2025
Draft Accounting Policies 2024/25 To present the Draft Accounting Policies 2024/25 to members for approval	Anna Crouch, Head of Finance	23 April 2025	Standards and Ethics Report - Quarter 4
Treasury Management Stewardship Report 2024/25 To report the Treasury Management Stewardship Report 2024/25 to members	Anna Crouch, Head of Finance	4 June 2025	Treasury Management Stewardship Report 2024/25 To report the Treasury Management Stewardship Report 2024/25 to members

NORTH WEST LEICESTERSHIRE DISTRICT COUNCIL

AUDIT AND GOVERNANCE COMMITTEE – WEDNESDAY, 7
AUGUST 2024

Title of Report	ANNUAL AUDIT OPINION	
Presented by	Kerry Beavis Audit Manager	
Background Papers	Public Sector Internal Audit Standards	Public Report: Yes
Financial Implications	None arising from this report	
	Signed off by the Section 151 Officer: Yes	
Legal Implications	None arising from this report	
	Signed off by the Monitoring Officer: Yes	
Staffing and Corporate Implications	None arising from this report	
	Signed off by the Head of Paid Service: 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.	

1.0 BACKGROUND

- 1.1 As set out in the Public Sector Internal Audit Standard (PSIAS) 2450, the Chief Audit Executive (Audit Manager) must provide an annual report to the board (Audit and Governance Committee) timed to support the Annual Governance Statement. This report and opinion should be considered as part of the evidence supporting the Annual Governance Statement.

Policies and other considerations, as appropriate	
Council Priorities:	A Well-Run Council
Policy Considerations:	None
Safeguarding:	None
Equalities/Diversity:	None
Customer Impact:	None
Economic and Social Impact:	None
Environment, Climate Change and Zero Carbon	None
Consultation/Community/Tenant Engagement:	The Director of Resources has been consulted.
Risks:	Non-compliance 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 2023/24

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 2023 to 31 March 2024 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 2023/24 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 2023/24

- 2.1 Resources both within the Internal Audit team and the areas audited have continued to cause difficulties during 2023/24, with audits being delayed or taking longer to complete due to availability of staff.

Internal audit continued to provide the additional support required for assurance on grants.

- 2.2 In line with the Public Sector Internal Audit Standards, Internal Audit has 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 2024, I am only able to give **limited assurance** on the overall control environment. To be consistent with 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 areas audited. As this is not a positive assurance overall the Corporate Leadership Team have developed an action plan in response 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 2023/24

3.1 The risk based internal audit plan for 2023/24 was presented and approved by the Audit and Governance Committee on 26 April 2023. 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 2023/24 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.	14
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		17

- 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. The internal audit service at the Partnership was provided by Mazars, there have been no audits reported for this service during 2023/24.
- 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 is updated 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 2023/24 is included at Appendix B. It must be noted that the majority of the recommendations have yet to reach their agreed implementation date.

4. ISSUES RELEVANT TO THE PREPARATION OF THE ANNUAL GOVERNANCE STATEMENT

- 4.1 The Internal Audit team has issued 14 audit reports with limited assurance during 2023/24. These should be considered when preparing the Annual Governance Statement:
- **Creditors**
The main areas identified for improvement were the timeliness of reconciliations, timeliness of processing supplier invoices and credit notes, availability of reporting functionality to carry out management checks.
 - **Debtors**
The main areas identified for improvement were the debtor reconciliations being completed in a timely manner, bad debt identification and write-off's, the introduction of consistent and timely reminder letters being issued.
 - **Main Accounting and Budgetary Control**
The main areas identified for improvement were the timely completion of reconciliations, timely and accurate compilation of budgetary information to budget holders, monitoring appropriate accounting of virements.
 - **Treasury Management**
The main areas identified for improvement included the reconciliations between treasury management and the general ledger, review of the designated officers detailed on the fidelity guarantee insurance, review of access to the software system.
 - **Housing Repairs**
The main areas identified for improvement included the management and monitoring of orders and variations, the procedure for the checking and approval of invoices, the process and management of recharges to tenants, appropriate recording of all inspections and surveys.
 - **Housing Planned Maintenance**
The main areas identified for improvement included the management and monitoring of contracts and payments, the completion and documentation of

inspections, the authorisation of variations to works, the review of processes to remove duplication of work.

- **Asbestos Management**
The main areas identified for improvement included having an approved Asbestos Management Plan in place, having an up-to-date Asbestos Register, the carrying out of assessments to confirm compliance with the Council's statutory duties relating to asbestos management.
- **Safeguarding**
The main areas identified for improvement included a review of the safeguarding referral process, monitoring and recording of Disclosure and Barring Service (DBS) rechecks, updating of the DBS policy and procedures, the recording of safeguarding risks within relevant risk registers.
- **Fleet Management**
The main areas identified for improvement are the approval of an asbestos management plan, maintaining records for the monitoring of the results of asbestos surveys, effective contract monitoring and the relevant training of officers across the Council.
- **Workforce Planning**
The main areas identified for improvement included the development of a workforce planning strategy.
- **Remote Support & Data Exchange**
The main areas identified for improvement included the need to ensure data transfers are completed adequately by service users, the update of the ICT and Cyber Security Policy to cover all key issues in relation to data transfers and remote support.
- **Cyber Security**
The main areas identified for improvement have been reported but as the report is confidential no further details have been included within this report.
- **Capital Programme Management**
The main areas identified for improvement included the availability of documented procedures and training for new managers, the virement procedure and the monitoring and reporting of capital projects.
- **Procurement and Contract Management**
The main areas identified for improvement included the completion and approval of the Council's procurement strategy, maintaining an up-to-date contract register, the management and monitoring of contracts is in place and documented across the Council.

There were no audit reports issued without any assurance during 2023/24.

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 process within a service area, 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 2023/24 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 Director of Resources (S151 Officer).
 - Customer satisfaction surveys were sent out to all Team Managers and/or Team Leaders who had an audit in their service area. Only two returns were received for 2023/24 both providing 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 Governance Committee on 20 January 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 has added value in the following ways:
- Providing assurance on various grants during the year.
 - 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 2023/24 the Internal Audit Shared Service conformed to the Public Sector Internal Audit Standards.

RESULTS OF INDIVIDUAL AUDIT ASSIGNMENTS AGAINST THE 2023/24 AUDIT PLAN

Audit Area	Type	Planned Days	Actual Days	Status	Assurance Level	Recommendations				Comments
						C	H	M	L	
Housing Repairs	Audit	40	43	Completed	Limited	-	4	16	3	
Housing Planned Maintenance	Audit	40	3.5	Completed	Limited	-	9	3	2	
Asbestos Management	Audit	10	12	Completed	Limited	-	11	1	-	
HMO	Audit	10	0.5	Completed	Reasonable	-	3	4	2	
Safeguarding	Audit	8	19.5	Completed	Limited	-	6	7	3	
Fleet Management & Operating License	Audit	8	12.5	Draft	Limited	-	19	2	-	
Treasury Management	Audit	4	4.5	Completed	Limited	-	5	1	-	
Debtors	Audit	10	10	Completed	Limited	-	7	4	1	
Creditors	Audit	10	11.5	Completed	Limited	-	9	5	-	
Main Accounting	Audit	10	11	Completed	Limited	-	8	4	-	
Rent Accounting	Audit	10	9	Draft	Reasonable	-	1	5	-	
Workforce Planning	Audit	10	7	Completed	Limited	-	3	-	-	
IT Asset Management	Audit	10	10	Completed	Reasonable	-	1	3	3	
Remote Support & Data Exchange	Audit	Contractor		Completed	Limited	1	4	4	-	
Cyber Security	Audit	Contractor		Completed	Limited	2	-	12	2	
Corporate Policy Management	Advisory	10	8.5	Completed	N/A					
Capital Programme Management	Audit	10	5	Completed	Limited	-	3	6	-	
Procurement & Contract Management	Audit	10	15	Completed	Limited	-	5	3	-	
Grant Assurance	Assurance		7	As required	N/A					

Recommendations key – see Appendix B

SUMMARY OF INTERNAL AUDIT RECOMMENDATIONS FOLLOW UP 2023/24

Internal Audit follows 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 monthly and any overdue and extended recommendations are highlighted to Audit Committee.

The table below shows the progress against recommendations made by Internal Audit during 2023/24. 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 2024/25, 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	3	3	-	-
High	98	10	87	1
Medium	80	20	59	1
Total	181	33	146	2

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 2023-24

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 2023, this includes Code of Ethics and Principles.	Annual
Customer satisfaction surveys	1311	Two received for 2023/24. 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 2023/24 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 Director of Resources (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 2023. 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, 7
AUGUST 2024

Title of Report	MANAGEMENT RESPONSE TO ANNUAL INTERNAL AUDIT OPINION 2023/24	
Presented by	Paul Stone Director of Resources	
Background Papers	Management Response to Internal Audit Opinion 2022/23 – Audit & Governance Committee 26 July 2023 NORTH WEST LEICESTERSHIRE DISTRICT COUNCIL NORTH WEST LEICESTERSHIRE DISTRICT COUNCIL NORTH WEST LEICESTERSHIRE DISTRICT COUNCIL	Public Report: Yes
Financial Implications	There are no direct financial implications to be considered.	
	Signed off by the Section 151 Officer: Yes	
Legal Implications	There are no direct legal implications arising from this report.	
	Signed off by the Monitoring Officer: Yes	
Staffing and Corporate Implications	There are no direct staffing or corporate implications arising from this report.	
	Signed off by the Head of Paid Service: Yes	
Purpose of Report	This report provides details of the Internal Audit Opinion 2023/24 and the Management Response to the findings.	
Recommendations	THAT THE COMMITTEE NOTES THE MANAGEMENT RESPONSE TO THE ANNUAL AUDIT OPINION 2023/24.	

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 2023/24 is set out on a separate item on the Committee's agenda.

1.2 The Opinion covers the overall adequacy and effectiveness of the Council's framework of governance, risk management and control. The draft Internal Audit Annual Opinion for 2023/24 is 'Limited Assurance'.

1.3 It is recognised that this is the second consecutive year that the opinion has been 'Limited Assurance' and that this is not acceptable and requires improvement. Before considering the management response to this year's opinion, the Committees attention is drawn to the progress on the action plan in response to the 2022/23 opinion. The action plan is attached to this report at Appendix One. Significant progress has been made in a number of areas identified on the action plan including:

:

- Internal audit recommendations are a standing item on the Corporate Leadership Team agenda.
- Statutory Officers discuss the recommendations with the Head of Internal Audit and where the recommendations are not being actioned in line with the timescales identified in the Audit, the Statutory Officers request that the Director and Head of Service attend the Statutory Officer meeting to provide further details of the actions being taken.
- Recruitment to key internal audit posts.
- Senior Leadership structure is now embedded with a Director of Resources (S151 Officer) joining the Council in September 2023.
- The Internal Audit Team have offered to attend team briefings to raise the profile of Internal Audit. The offer will be extended into 2024/25 to further encourage and enable teams to meet with Internal Audit to understand their role.
- Project management guidelines and templates developed and available for all staff. Project management training is also scheduled for September 2024, together with an e-learning module which has been developed and is to be published shortly.
- The Director of Resources and Internal Audit Manager have worked with the Audit and Governance working group on a programme of training and development for the Committee. This has included sessions on risk management, accounts, internal audit progress reports and standards and ethics reports.
- An extensive programme of training on Governance has been delivered to all managers across the Council
- The Council has been recognised by the Local Government Association for its approach to Governance and Assurance for the changes it has implemented.

1.4 A further action was to appoint an Independent Member of the Audit and Governance Committee. Whilst the Council has advertised the position on two occasions, there has been no interest. However, the requirements for the role have been updated and social media and other media will be used to advertise the role more widely to reach a broader audience.

2.0 MANAGEMENT RESPONSE AND ACTIONS

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 is 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 Following the issuance of the Opinion, and with an understanding of the circumstances under which it was formulated, a special meeting of the Corporate Leadership Team convened on 26 June 2024 to discuss the contents of the Opinion. The actions agreed are set out below.

Planned Actions

2.3 The Audit and Governance Committee is provided with internal audit reports that are deemed to have limited or no assurance. In instances where a report is assigned this opinion, the respective Director and Head of Service are required to present before the Audit and Governance Committee, detailing the measures they are implementing in response to the recommendations. In the context of governance, the attendance of Heads of Service at this Committee meeting is a crucial step in ensuring accountability and transparency. These meetings serve as a platform for leaders to present the actions they have taken in response to recommendations made by previous audits. It is an opportunity for them to articulate their strategies, progress, and any challenges they face in implementing changes. If there has been no progress, it is equally important for them to explain the reasons, whether they are due to resource constraints, shifting priorities, or unforeseen complications. This process not only holds Directors and Heads of Service accountable but also provides valuable insights into the operational aspects of the Council, fostering a culture of continuous improvement. The Committee can then assess the validity of the explanations provided and offer appropriate challenge and guidance.

2.4 The Council's Statutory Officers have agreed in principle to enhancing Internal Audit capacity. To maintain consistent auditing of the Council's services and to guarantee thorough implementation of recommended actions, it has been decided to recruit an extra officer for the Internal Audit team. A proposal for additional resources will be presented during the budget setting process for the 2025/26 financial year for consideration by Members.

2.5 The Internal Audit team will keep detailed records of implemented audit recommendations to demonstrate progress and direction. This documentation will serve as a clear indicator of the improvements made and the ongoing journey towards improved audit opinions within services.

2.6 A dedicated meeting of the Corporate Leadership Team (CLT) will be held in August to focus exclusively on Internal Audit processes. This dedicated session will allow for discussion of Internal Audit's contribution to the governance of the Council. Subsequently, the CLT will convene monthly, dedicating these sessions exclusively to the discussion of recommendations from internal audits.

2.7 There will be a renewed focus on the Internal Audit function which will be achieved through:

- Stakeholder engagement –educating Council's officers on the role of Internal Audit. This includes explaining their role in evaluation the effectiveness of risk management, control and governance processes.

- Demonstrating value – showing how internal audit can help the Council. This could be through risk-based auditing, aligning internal audit assurance and advice to the Council's strategic risks and priorities.
- Enhanced reporting – ensuring the information within audit reports tells the story of the internal audit opinion.
- Working with the Audit and Governance Committee – the presence of an audit committee can enable a higher profile for internal audit, clearer reporting lines, additional assurances that internal audit reports would be acted upon, and independent monitoring of audit performance.

2.8 Internal audits are currently conducted on a by-exception basis focusing primarily on areas with significant risks or where problems have been previously identified. This approach allows auditors to concentrate their efforts on the most critical aspects of the Council's operations, ensuring that resources are used efficiently. However, it's important to note that while this method is effective for pinpointing issues, it may overlook areas where services are performing well. By acknowledging the good work being done, the Council can motivate staff, reinforce positive behaviour, and foster an environment of continuous improvement.

2.9 An Action Plan has been developed to monitor progress, a copy of which is shown at Appendix Two. 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.

3.0 Summary

3.1 Management has recognised the necessity to prioritise the improvement of internal audit reports that have been categorised as 'limited assurance.' A proactive approach is essential to enhance this area.

3.2 The issuance of numerous limited assurance reports is concerning but is not unexpected given the specific ask of Internal Audit to focus specifically on those areas where senior management have identified risks. It is important to note, also, that the Council is navigating through several well-known sectoral and national challenges that are not unique to North West Leicestershire. These include issues with staff recruitment and retention, as well as ongoing recovery from the impacts of Covid-19. Housing remains an area with significant capacity constraints, yet the establishment of the Housing Improvement Board provides oversight of future developments including a more onerous regulatory environment. The Committee has been kept informed by the Director of Resources about the challenges faced by the Finance Team, which were also detailed in a comprehensive letter to Committee members.

3.3 The Committee Members can be confident that a substantial number of audit recommendations have been successfully actioned over the past year. This progress is a testament to Management's commitment to continuous improvement. Presenting detailed information, as highlighted in paragraph 2.5 above, on the volume and schedule of these implementations will provide the Committee with valuable insights into the direction of travel of the Council's processes and governance.

Policies and other considerations, as appropriate	
Council Priorities:	- A Well-Run Council
Policy Considerations:	Not applicable.

Safeguarding:	Not applicable.
Equalities/Diversity:	Not applicable.
Customer Impact:	Not applicable.
Economic and Social Impact:	Not applicable.
Environment, Climate Change and Zero Carbon	Not applicable.
Consultation/Community/Tenant Engagement:	In developing the Action Plan there has been engagement with Statutory Officers, the Corporate Leadership Team and the Internal Audit Manager.
Risks:	The Council's governance arrangements are a critical part of its operations to ensure decision making is robust and effective. Internal audit is an important part of these governance arrangements. 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.
Officer Contact	Paul Stone Director of Resources paul.stone@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	Status
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 and Governance Committee on 26 April 2023	Progress on delivery of the Plan is reported to CLT and A&G Committee throughout year	March 2024	Internal Audit Manager	Ongoing – quarterly reports have been provided to CLT and A&G	Completed
		Internal Annual Report for 2023/24 to provide final performance	July 2024		Annual Audit Opinion 2023/24 for consideration at meeting of Audit and Governance on 7 August 2024.	Completed
		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			Completed

<p>Strengthen performance management process for implementation of internal audit recommendations</p>	<p>Initial conversations between Statutory Officers and Internal Audit Manager have established initial improvements</p>	<p>Fully review current IA Recs implementation performance management process</p>	<p>Sept 2023</p>	<p>Director of Resources</p>	<p>Internal Audit Recommendations are reviewed by CLT monthly. Audit Committee may ask Heads of Service/Directors to attend meetings where recommendations fail to be implemented.</p>	<p>Completed</p>
---	--	---	------------------	------------------------------	--	------------------

Action	Current Status Position	Work to Fully Implement Action	Timeline for Delivery	Lead Officer	Comments	Status
					<p>The process for consideration of Internal Audit Recommendations and their subsequent implementation has been reviewed. Departmental and Directorate management meetings will consider Internal Audit recommendations. If there appears to be a failure to implement recommendations these will be considered at the Statutory Officer meeting and subsequently at CLT, and Audit and Governance Committee if required.</p>	
		Assign audit recommendations to the officer responsible for implementing them	July 2023	Internal Audit Manager		Completed

		Internal Audit to attend Team meetings at least six monthly. [Head of Service to invite Internal Audit. Internal Audit to produce record of meeting]	Sept 2023	Head of Service / Team Manager	IA has been invited to two meetings – Housing in July 23 and Community Services 24/10/23. The IA Manager is a member of the Legal and Support Services Management Team and attends Management Team Meetings. No further requests to attend meetings have been received.	Invites have been limited.
--	--	--	-----------	--------------------------------	---	----------------------------

Action	Current Status Position	Work to Fully Implement Action	Timeline for Delivery	Lead Officer	Comments	Status
		Enhanced initial process - statutory officer sessions for recommendation owners to justify their plan for delivery of recommendations	July 2023	Director of Resources	Standing item at CLT meetings. Monthly Statutory Officer meeting will also review as appropriate.	Completed
		Attendance at Audit and Governance Committee for CLT Lead to report progress on delivery. On an exception basis for late or extended recommendations.	Sept 2023	Director of Resources	See above.	Completed
Strengthen reporting process to Audit & Governance for internal audit recommendations		Review the reporting process	Sept 2023	Director of Resources	Recommendations list is now part of the Statutory Officers monthly meeting.	Completed
		Implement enhanced exception reporting (with focus on extensions and missed deadlines) for recommendation owners with Statutory Officer and at Audit & Governance Committee	December 2023		Statutory Officer meetings to discuss recommendations have been scheduled.	Completed

		Embed the new process into the Council's way of working	March 2024		See above.	
Increased capacity of internal audit resources / team	<ul style="list-style-type: none"> ○ A review of the team was undertaken in Autumn of 2022. ○ A new structure was agreed by all partner Council's. ○ NWL agreed additional resources as part of its 2023/24 base budget in February 2023. ○ Recruitment to the new structure has commenced with the successful appointment of an Apprentice role 	Fully recruit to new Internal Audit structure. Currently there is one post in the process of recruitment.	Sept 2023	Internal Audit Manager	See above re – staffing. Trying to source agency support to enable the plan to be implemented.	Completed

Action	Current Position	Status	Work to Fully Implement Action	Timeline for Delivery	Lead Officer	Comments	Status
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 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 and commenced in September 2023.	n/a	n/a	n/a	n/a	Completed	Completed
Improve synergies and linkages between internal and external audit			Internal Audit to have regular meetings with External Audit	October 2023	Internal Audit Manager	Relationship to be developed with new auditors Azets	Ongoing
Raise the profile and importance of internal audit in the Council	<ul style="list-style-type: none"> o Senior management o recognises that internal audit is important to ensure the Council performs effectively. The 		The importance of internal audit to staff is communicated to all staff as part of the overall governance framework of the Council by including an	December 2023	Head of Legal and Support Services	Training provided during w/c 9 October 2023. Further governance training delivered in respect of procurement, decision making, finance and	Completed

	<p>senior leadership team has been strengthened.</p> <ul style="list-style-type: none"> Additional capacity has been secured for the Internal Audit team. Reference to role of Internal Audit was included in CLT blog in June 2023. 	<p>Internal Audit module in the annual corporate governance training</p>			<p>information governance. Training will take place annually.</p> <p>Governance training scheduled for November 2024.</p>	
		<p>Review Internal Audit training on their function/role on Skillgate</p>	<p>March 2024</p>	<p>Internal Audit Manager</p>	<p>Face to face training carried out on 11/10/23 for CLT and Team Managers, also open to all other staff, as part of the governance training. Consideration being given to adding something on to Skillgate. IA currently reviewing and updating the fraud module. on Skillgate, this will then become a mandatory training module for all staff to complete on an annual basis starting April 2024.</p>	<p>Completed</p>

		<p>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</p>	<p>December 2023</p>	<p>Directors</p>	<p>Statutory Officers have agreed that departments will complete a departmental assurance framework to support this. Template to be developed by the Director of Resources.</p>	<p>Completed</p>
		<p>Internal Audit included as part of the decision making/grant bids/project set up process</p>	<p>March 2024</p>	<p>Directors and Heads of Service</p>		<p>Ongoing</p>
		<p>Review project management templates, toolkit, and guidance to include input from/</p>	<p>March 2024</p>	<p>Director of Resources</p>	<p>Project management policy and templates have been published.</p>	<p>Completed</p>

Action	Current Status Position	Work to Fully Implement Action	Timeline for Delivery	Lead Officer	Comments	
		engagement with Internal Audit			Information to be cascaded across the Council.	
		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 and OD	The service plans templates are in the process of being finalised and will incorporate this action.	Not completed.
		Engage internal audit as part of Business/Service Plan process	March 2024	Directors/Heads of Service		Not completed.
		Consider if managers' Job Description need to be updated to reflect importance of assurance.	March 2024	Head of HR and OD		Not completed.
		Consider if the staff appraisal process could assist in managing implementation of internal audit recommendations.	September 2023	Head of HR and OD	The annual review guidance is being updated to point managers to the internal audit considerations.	Completed
		Internal Audit to produce regular blogs, including case studies of usefulness of early/proactive engagement	March 2024	Internal Audit Manager	No changes yet due to staffing resources.	Not completed.

Appendix One

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	A review of the IA intranet page has started. It is intended to fully revamp this page with a new look and more information.	Not completed.
		Implement the findings of the review	December 2023		See above.	Not completed.
Implementation of the Council's new	The new finance system was implemented and	n/a	n/a	n/a		Completed

Action	Current Status Position	Work to Fully Implement Action	Timeline for Delivery	Lead Officer	Comments	
finance system to enhance financial control environment	went live from 1 April 2023. This will improve financial assurance from an internal audit perspective.					
Meetings between Internal Audit Manager and the Chair of the Audit Committee		Set up regular meetings	July 2023	Internal Audit Manager	Meetings arranged to follow the committee pre-meets. Completed	Completed.
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 ○ Member Working Party established and had their first meeting. ○ Training sessions for Members took place on Role of Audit Committee (5 June) and Treasury Management Training (6 July) 	Developing the training plan by working group	Oct 2023	Director of Resources	Training completed in early October.	Completed.
		Delivery of the training plan	On-going			Completed.
		Appointment of independent persons on the Audit & Governance	Oct 2023		Currently being advertised with a closing date of 16 August 2024.	Ongoing.

This page is intentionally left blank

Management Actions in Response to Annual Internal Audit Opinion 2023/24

Action	Current Status	Timeline for Delivery	Responsible Officer	Comments
Heads of Service to attend Audit and Governance meetings to respond to queries in respect of 'limited assurance' or 'no assurance' opinions.	Head of HR, Head of Finance and Head of Housing to attend Audit and Governance Committee on 7 August 2024	Ongoing	Statutory Officers	
Additional resource for Internal Audit	Proposal included within draft budget proposals for 2025/26 for consideration as part of budget process.	February 2025	Internal Audit Manager	
Further information to be provided by Internal Audit to show the direction of travel on audit recommendations.	Process is being reviewed by the Internal Audit Manager.	September 2024	Internal Audit Manager	
Continued focus on the Internal Audit function. This includes: <ul style="list-style-type: none"> Dedicated monthly Corporate Leadership Team (CLT) meeting to focus on audit recommendations. Requests for extension of audit deadlines to be made at the CLT meeting. Statutory Officers to request separate meetings with Directors/Heads of 	The CLT meetings are scheduled in diaries.	December 2024	Statutory Officers	

<p>Service for any areas of concern.</p> <ul style="list-style-type: none"> • CLT to discuss the annual audit plan in draft in March each year. • Directors to discuss progress against audit recommendations at performance meetings. • Internal Audit to provide further detail/training on the work of Internal Audit to CLT • Internal Audit Manager to provide details of how she arrives at the audit opinion for each report 				
<p>Acknowledgement of good work by services within audit reports.</p>		<p>December 2024</p>	<p>Internal Audit Manager</p>	
<p>Appointment of an independent Audit Committee Member.</p>	<p>The role is currently out to advert with a closing date of 16 August 2024.</p>	<p>December 2024</p>	<p>Director of Resources</p>	
<p>A suite of governance training has been arranged for November 2024.</p>		<p>November 2024</p>	<p>Head of Legal and Support Services</p>	
<p>Actions brought forward from 2022/23 Action Plan</p>				
<p>Internal Audit to attend Team meetings at least six monthly. [Head of Service to invite Internal Audit. Internal Audit to produce record of meeting]</p>		<p>December 2024</p>	<p>Internal Audit Manager</p>	

Internal Audit to have regular meetings with External Audit		December 2024	Internal Audit Manager	
Internal Audit Included as part of the decision making/grant bids/project set up process		March 2025	Head of Internal Audit	
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 2024	Head of HR and Organisational Development	
Engage internal audit as part of Business/Service Plan process		December 2024	Directors/Heads of Service	
Consider if managers' Job Description need to be updated to reflect importance of assurance.		December 2024	Head of HR and Organisational Development	
Internal Audit to produce regular blogs, including case studies of usefulness of early/proactive engagement		December 2024	Internal Audit Manager	
Review the current intranet presence and accessibility for Internal Audit		December 2024	Internal Audit Manager	

This page is intentionally left blank

NORTH WEST LEICESTERSHIRE DISTRICT COUNCIL

AUDIT AND GOVERNANCE COMMITTEE – WEDNESDAY, 7
AUGUST 2024

Title of Report	INTERNAL AUDIT PROGRESS REPORT	
Presented by	Kerry Beavis Audit Manager	
Background Papers	Public Sector Internal Audit Standards Internal Audit Plan 2024/25	Public Report: Yes Appendix 2 is exempt under Paragraph 3 of Part 1 of Schedule 12A to the Local Government Act 1972
Financial Implications	None arising from this report	
	Signed off by the Section 151 Officer: Yes	
Legal Implications	None arising from this report	
	Signed off by the Monitoring Officer: Yes	
Staffing and Corporate Implications	None arising from this report	
	Signed off by the Head of Paid Service: Yes	
Purpose of Report	To inform the Committee of the progress against the Internal Audit plan for 2024/25 and to highlight any incidences of significant control failings or weaknesses that have been identified.	
Recommendations	THAT THE AUDIT AND GOVERNANCE COMMITTEE NOTES 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 2024/25 Audit Plan on 24 April 2024. The Committee receives quarterly progress reports.

2.0 PROGRESS REPORT

2.1 The Internal Audit Progress Report for quarter 1 is attached at Appendix 1. A confidential audit report is attached at Appendix 2.

Policies and other considerations, as appropriate	
Council Priorities:	An effective internal audit service supports all council priorities.
Policy Considerations:	N/A
Safeguarding:	There are no specific risks associated with this report.
Equalities/Diversity:	N/A
Customer Impact:	N/A
Economic and Social Impact:	N/A
Environment, Climate Change and Zero Carbon	N/A
Consultation/Community/Tenant Engagement:	The report was presented to Corporate Leadership Team on 26 June 2024
Risks:	There are no specific risks associated with this report, however, if the Audit and Governance Committee did not receive periodic reports from Internal Audit, there would be a risk of none conformance 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 Progress Report 2024/25 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 2024/25 Internal Audit Plan up to 30 June 2024.

2. Internal Audit Plan Update

- 2.1 The majority of the first quarter has been focused on the completion of the 2023/24 audit plan. Delays in completing the plan have been due to staffing issues within both the audit service and services being audited. There have been fourteen audit reports issued since the last report. Due to the number of reports, it has been agreed that the following will be discussed at the Audit and Governance Committee meeting on 7 August 2024 -

- Housing Repairs
- Housing Planned Maintenance
- HMO's
- Asbestos Management
- Remote Support and Data Exchange
- Cyber Security – CONFIDENTIAL

Summaries of the reports are detailed in appendix B.

The remaining audit reports, detailed below, will be discussed at the Audit and Governance Committee meeting on 22 August 2024 -

- Creditors
- Debtors
- Main Accounting and Budgetary Control
- Treasury Management
- Safeguarding
- Workforce Planning
- Capital Programme Management
- Procurement and Contract Management

- 2.3 The 2024/25 audit plan is included at Appendix A for information.

3. Internal Audit Recommendations

- 3.1. Internal Audit monitor and follow up critical, high and medium priority recommendations. There are currently no overdue recommendations. Further details of extended recommendations are detailed in Appendix C for information.

Year	Not Due		Extended		Overdue	
	High	Medium	High	Medium	High	Medium
21/22	-	-	5	1	-	-
22/23	-	-	9	5	-	-
23/24	65	50	3	-	-	-

4. Internal Audit Performance Indicators

- 4.1. Progress against the agreed Internal Audit performance targets is documented in Appendix D.

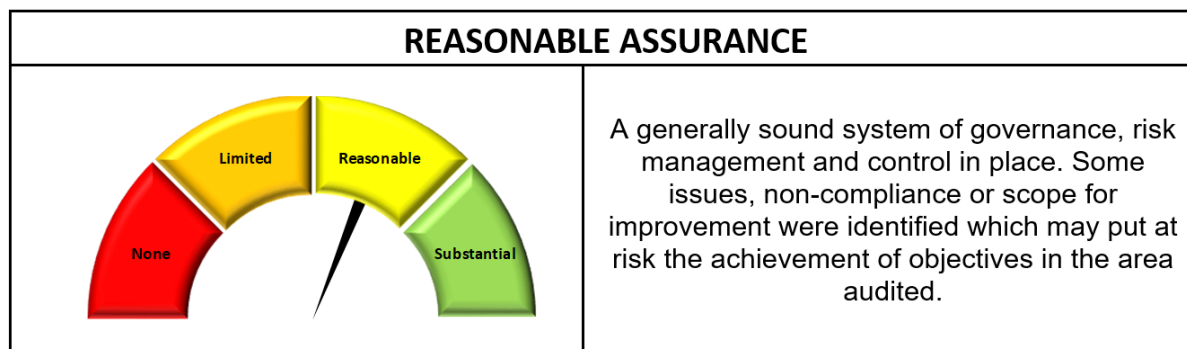
2024/25 AUDIT PLAN AS AT 30 JUNE 2024

Audit Area	Type	Planned Days	Actual Days	Status	Assurance Level	Recommendations				Comments
						C	H	M	L	
Housing	Audit	30		To be agreed						
Housing Compliance	Audit	20		Q3						
Housing Contract Management	Audit	15		Q2						
Housing Stocktakes	Audit	2		To be agreed						
Tree Stock Management	Audit	8	0.5	Engagement Planning						
Waste Services	Audit/ Advisory	20		To be agreed						
Insurance	Audit	8	0.5	Engagement Planning						
VAT & Benefits in Kind	Audit	10		Q2						
Key Financial Systems	Audit	55		Q3,4						
Regeneration Projects	Consultancy	20	12	In progress						
IT Audits	IT Audit Contractor	20		To be agreed						
Net Zero	Audit	8		Q3						
Driver Checks	Advisory	6	0.5	In progress						
Transformation Projects	Advisory	3		As required						
Complaints	Audit	12		Q2						
UKSPF	Audit	8		Q2						To be moved to Q3
Changing Places	Grant	2		Q3						To be moved to Q3
Procurement & Contract Management	Audit	12		Q4						
Outstanding from 23/24										
Fleet Management	Audit	8	14	Draft	Limited	-	19	2	-	
Asbestos Management	Audit	10	12	Complete	Limited	-	11	1	-	
Debtors	Audit	10	10	Complete	Limited	-	7	4	1	

Creditors	Audit	10	10	Complete	Limited	-	9	5	-	
Main Accounting	Audit	10	10	Complete	Limited	-	8	4	-	
Treasury Management	Audit	8	7	Complete	Limited	-	5	1	-	
Housing Repairs	Audit	40	51	Complete	Limited	-	4	16	-	
Housing Planned Maintenance	Audit	40	24	Complete	Limited	-	9	2	1	
HMO's	Audit	10	7.5	Complete	Reasonable	-	3	4	2	
Safeguarding	Audit	8	20.5	Complete	Limited	-	6	7	3	
Workforce Planning	Audit	8	5.5	Complete	Limited	-	3	-	-	
Remote Support & Data Exchange	Audit	10	10	Complete	Limited	1	4	4	-	
Cyber Security	Audit	10	10	Complete	Limited	2	-	12	2	
Capital Programme Management	Audit	10	5.5	Complete	Limited	-	3	6	-	
Procurement & Contracts	Audit	10	15	Complete	Limited	-	5	3	-	
Rent Accounting	Audit	10	9	Draft	Reasonable	-	1	5	-	

SUMMARY OF FINAL AUDIT REPORTS ISSUED DURING 2024/25 Q1 FOR DISCUSSION AT THE 7 AUGUST MEETING

HMO's



52

Key Findings

Areas of positive assurance identified during the audit:

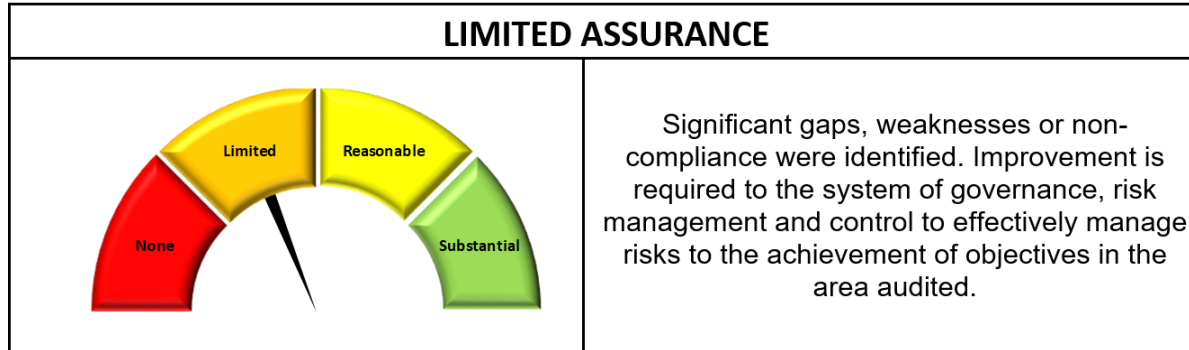
- Policies and procedures are available to all relevant staff.
- HMO fees have been approved and published as required and income due is collected.
- Officers are suitably qualified.

The main areas identified for improvement are:

- The recording of verification checks and retention of documents.
- The checking of applications.
- The scheduling and completion of interim inspections.

Recommendation	Priority	Response/Agreed Action	Officer Responsible	Implementation Date
1. The internal procedure is revised to include the requirement to consider the Article 4 Direction for relevant applications.	Medium	Agreed.	Environmental Protection Team Manager	September 2024
2. Service managers are reminded annually of the requirement to publicise the revised fees and charges relating to their service area.	Medium	Agreed	Anna Crouch – Head of Finance	February 2025
3. The discrepancy in respect of the information relating to the number of self-contained units is investigated and resolved to ensure that all details are accurately recorded on the Public Register.	Medium	Agreed. To be actioned after the next system update which is due in Jun-24.	Systems Support Officer.	August 2024
4. A consistent document retention procedure is agreed, documented and communicated to all relevant staff.	Medium	Agreed.	Environmental Protection Team Manager	September 2024
5. Officers are reminded that all verification checks must be recorded and supporting evidence retained where required.	High	Agreed.	Public Protection Team Leader	June 2024
6. A supervisory checking process is introduced to ensure that applications are processed correctly, and all key documents have been provided and retained on file before a licence is issued.	High	Agreed.	Environmental Protection Team Manager	September 2024 and ongoing.
7. The system case records of all current licences are checked and updated as required to confirm that the next inspection due has been scheduled (and completed where applicable) in accordance with the relevant risk assessment.	High	Agreed.	Public Protection Team Leader	July 2024

Remote Support & Data Exchange



The level of assurance indicated is as a result of the critical and high recommendations made in respect of controls reviewed. The critical issue was addressed during the course of review. These have not been re-visited / tested.

54

Key Findings

Areas of positive assurance identified during the audit:

- A policy has been drawn which relates to these two key areas (ICT and Cyber Security Policy) and has been approved by management. There is, though, a need to enhance these to cover some other key issues. Internal audit are currently completing a review of the Policy framework at the Council and will be making corporate recommendations accordingly.
- Steps have been taken to deploy the TeamViewer solution to manage remote third party connections. Some suggested additional controls have been recommended to enhance management controls including monitoring.
- It is understood a piece of work is planned relating to the Information Governance Framework in 2024. This is noted, however, some tasks may need to be completed urgently given our findings.

The main areas identified for improvement are:

- There is an urgent need to ensure data transfers are being completed adequately where they are being undertaken by service users.
- The ICT and Cyber Security Policy needs to be enhanced to cover all key issues.
- Key tasks need to be completed regarding Data Transfers. Briefly these are:

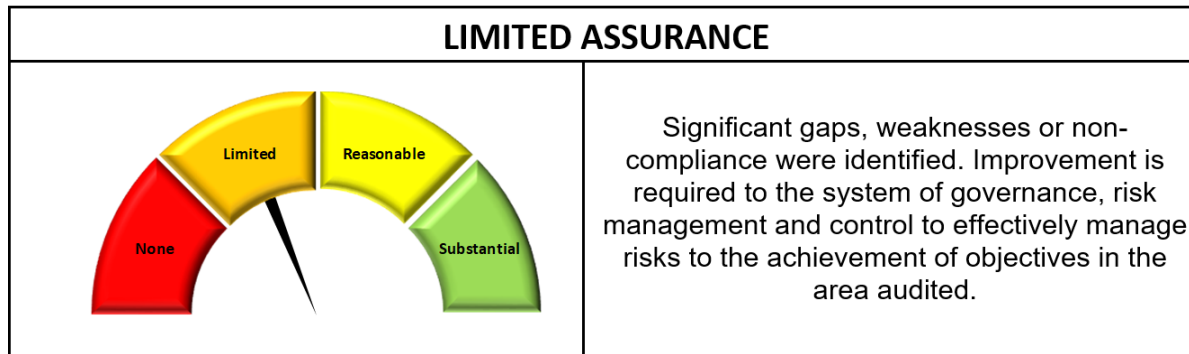
- Need to provide corporate guidance.
- Maintain a corporate register of data transfers.
- Ensure DPA risk assessments are in place, and reviewed periodically, for data transfers.
- Ensure appropriate agreements / contracts exist for data transfers undertaken.
- Key tasks need to be completed regarding remote third-party connections. Briefly these are:
 - Review available settings for the TeamViewer solution and activate key controls.

Recommendation	Priority	Response/Agreed Action	Officer Responsible	Implementation Date
<p>1.The IT Manager should look to enhance the ICT and Cyber Security Policy to cover the following:</p> <p><u>Remote Support Third Parties (2.1 Identification of Risks from Third Party Connections)</u></p> <ul style="list-style-type: none"> ➤ Reference should be made to any data accessed / viewed or downloaded. ➤ That ICT use management / audit logs to monitor activity. ➤ Destruction / retention of data requirements. ➤ Removal of access rights for remote support including any additional actions expected / required should this be necessary. <p><u>Data Exchanges 6.8 Data and Software Exchange</u></p> <ul style="list-style-type: none"> ➤ Should reference preferred method of transfer, security considerations including provision of security information i.e. encryption / password parameters. ➤ Electronic transfers need to be added and in greater detail and should cover user responsibilities, messaging and need for suitable agreements / contracts. ➤ Risk assessment requirement should be updated to reference electronic transfers. Currently it only states need for hardware access. <p>Reference to the “Records Management Officer” should be updated accordingly.</p> <p>Internal Audit have / are currently reviewing the Policy framework at the Council and will be making corporate recommendations accordingly.</p>	Medium	ICT and Cyber Security policy will be updated to reflect the recommendation. Data protection officer will be included to review the policy in terms of data exchanges/ protection.	ICT Team Manager and Data Protection Officer	September 2024
<p>2.A corporate register of data transfers should be documented and maintained. This should include a process for new data transfers to be notified to a nominated lead.</p>	Medium	The Council holds a Data Sharing Agreements Register. This will be reviewed and updated as part of the Information Governance Review to ensure that the information required is included.	Data Protection Officer	January 2025

<p>3.Steps should be taken to ensure risk assessments are in place for all data transfers in operation. Going forward it should be a requirement that all data transfers are risk assessed prior to operation. This should be prepared by the users in the directorates and approved by senior management. Once complete it should be communicated to the Data Protection Officer / other stakeholders as necessary.</p>	High	<p>The Council carries out Data Protection Impact Assessments. The process and guidance for these will be reviewed and updated as part of the Information Governance Review to ensure that staff are aware when such an assessment is required.</p>	Data Protection Officer	January 2025
<p>4.ICT management to review settings relating to the following:</p> <ul style="list-style-type: none"> ➤ Ensure any security related settings / parameters are set to support agreed policy. ➤ To review the access for users defined to some of the functionality available. ➤ Ensure alerting is enabled, where available, to notify any significant issues relating to use / connections made. These should be forwarded automatically to key ICT staff. ➤ Review the available management / audit log enabling this for significant events. ICT management should ensure that if a user ID is deleted from the TeamViewer solution such a deletion does not undermine the integrity of the log data i.e. that user's data is "lost". <p>Going forward ICT management will need to ensure these settings are documented accordingly and reviewed on a regular basis and evidenced.</p>	Medium	<p>Configuration settings in team viewer will be reviewed, to reflect the recommendation where possible.</p> <p>TeamViewer policy for 3rd party access will also be updated to reflect the changes</p>	ICT Services Support Manager	June 2024
<p>5.ICT process document (<i>TeamViewer - Use For 3rd Party Support</i>) should be reviewed and enhanced to ensure it supports the agreed approach for security and cover other work / tasks to be carried out by ICT staff in relation to the remote support work for third parties.</p>	Medium	<p>Will be reviewed in conjunction with the above recommendation</p>	ICT Team Manager	June 2024
<p>6.Appropriate controls should be confirmed for any data transfers being undertaken elsewhere in the Council.</p>	Critical	<p>Agreed. This has been implemented and only data is only sent through secure sources.</p>	FINANCE & IT	Implemented

<p>7.Steps should be taken urgently to ensure any users involved in data transfers are provided with guidance. As a minimum this should be issued to users, undertaking data transfers, to address the following:</p> <ul style="list-style-type: none"> ➤ Roles and responsibilities of all parties. ➤ Protection of data including security requirements for passwords used. ➤ Transmission of security related information. ➤ Covering messages regarding transmissions and key responsibilities. ➤ Use of checklists to ensure all tasks are completed as required. ➤ Storage of any “local” data retained and retention including destruction. ➤ Need for local procedures to be documented. 	High	<p>A procedure on the data protection aspects of information sharing has been drafted as part of the Information Governance Review and was shared as part of the audit. This procedure can be reviewed by the IT Manager to add any technical requirements. The procedure will be launched as part of the wider Information Governance Toolkit.</p>	<p>Data Protection Officer and ICT Team Manager</p>	<p>January 2025</p>
<p>8.Urgent steps should be taken to ensure the agreement / contract for the provision of the Market Harbough District Council has been signed and is in force. Steps should be taken to ensure the agreement / contract cover all key areas.</p>	High	<p>Agreed. This is currently being reviewed.</p>	<p>Interim Exchequer Services Team Leader</p>	<p>September 2024</p>
<p>9.A contract / agreement should be put in place for all external data transfers being undertaken. Such a contract / agreement should be subject to an annual review or should the recipient / provider of data change.</p>	High	<p>The draft procedure for information sharing, shared as part of the audit, sets out when a data sharing agreement or data processing agreement is required. The Council has template agreements for this purpose (also shared as part of the audit) but it may be appropriate in other circumstances to use a standard template provided by another party. Each agreement will be reviewed in accordance with its terms based on what is appropriate on a case-by-case basis.</p>	<p>Data Protection Officer</p>	<p>January 2025</p>

HOUSING PLANNED MAINTENANCE



Key Findings

Areas of positive assurance identified during the audit:

- There are appropriate five-year work programmes in place for home improvement works and cyclical painting.

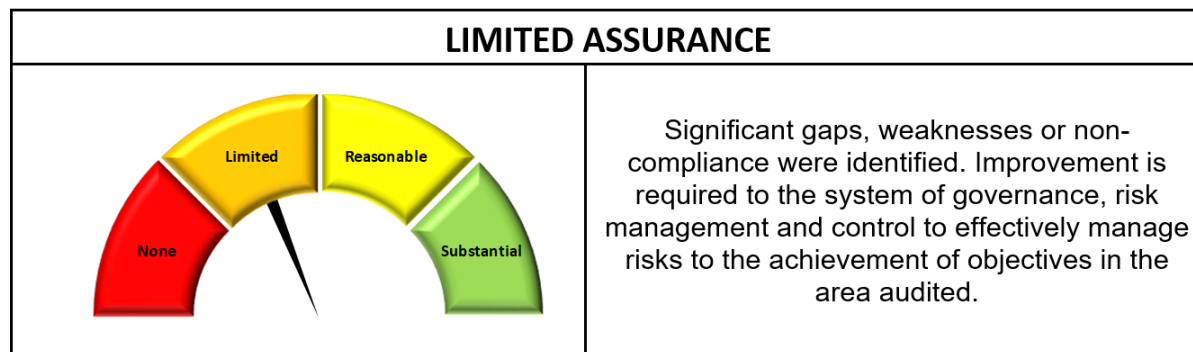
The main areas identified for improvement are:

- Key procedures are documented and made accessible to staff.
- Service processes and documentation to manage, record and monitor progress against the annual programme are aligned, with any duplication being removed.
- Variations are appropriately costed and authorised prior to work being undertaken.
- Relevant inspections are completed, recorded and documentation retained.
- Certificates and key documentation are received prior to completion sign off.
- Snagging works are identified and monitored.
- The consolidated invoice process is reviewed to ensure that there is a clear and transparent audit trail in place.
- Contracts are managed and monitored.

Recommendation	Priority	Response/Agreed Action	Officer Responsible	Implementation Date
1. All key procedures are documented and made accessible to staff, these should support relevant policies and tenancy guides.	Low	Work has commenced on reviewing the procedures. Since the Audit, a restructure has been actioned which changes the responsibilities between teams. Once this is completed the end-to-end process will be updated. Details given to operatives have already been operationally updated.	Head of Housing	April 2025
2. Management considers the use of a single source to manage, record and monitor progress against the annual programme to remove duplication in work and avoid error.	Medium	Agreed in principle, this will be reviewed once a full complement of Senior Management Team is in place.	Head of Housing	September 2025
3. Schedule of rates basket prices are reviewed to ensure they fully reflect actual costs.	Low	A recognised schedule of rates is used, it has just not been updated in line with the National Housing Federation (NATFED). The schedule of rates will be reviewed at the time a full system review is carried out.	Head of Housing	April 2025
4. The procedures and system parameters are reviewed to ensure orders and variations are appropriately costed and authorised. 8	High	An action plan will be put in place to address issues, but these actions will not be able to be addressed until a full complement of Senior Management Team is in place.	Head of Housing	April 2025
5. The authorising of variations and orders through the Versa system is investigated to ensure an adequate audit trail exists.	Medium	Discussions will be held with Versa to identify where the audit trail is and if this issue can be resolved.	Housing Strategy & Systems Team Manager	November 2024
6. Procedures and processes are put in place to ensure relevant inspections are completed, documentation is retained, and completion is evidenced on the housing management system (QL).	High	Post inspections are now being carried out by the asset team. Asbestos information is currently being addressed with the contractor to enable relevant users to access the information. This will be reviewed once a full complement of Senior Management Team is in place.	Head of Housing	April 2025
7. Processes are put in place to ensure certificates are obtained upon completion and are filed appropriately for future reference.	High	The reconciliation will, going forward, be carried out by the financial Asset Management Support Officer (AMSO).	Support Services Manager	October 2024

		The process has been confirmed as – the in-house team complete compliance via a tablet. Contractors send through compliance certificates which are uploaded to the MRI software system with relevant reference number. Audit to review in three months to ensure process is now working.		
8. Processes are put in place to ensure snagging works are identified, recorded and monitored to ensure remedial works are completed.	High	Agreed in principle, this will be reviewed once a full complement of Senior Management Team is in place.	Head of Housing	April 2025
9. A review of the process is undertaken and documented to ensure that there is a clear and transparent audit trail in place and the process is relatively managed and monitored, and all officers are aware of the responsibilities in relation to authorisation and payment processes.	High	Agreed in principle, this will be reviewed once a full complement of Senior Management Team is in place and the financial architecture is in place to support this.	Head of Housing	April 2025
10. The complexity of the spreadsheets being used are reviewed and the process is documented to for business continuity purposes. Additionally, any duplication of work should be removed.	High	Agreed in principle, this will be reviewed once a full complement of Senior Management Team is in place.	Head of Housing	April 2025
11. All documentation is stored on the housing shared drive to ensure data is secure, accessible and provides sufficient business continuity should officers leave.	High	This has been fully resolved and the approach of personal drive use has ceased.		Implemented
12. Housing contracts are made accessible to all appropriate officers.	High	A team's site has been set up within housing that holds copies of the contracts for all contracts going forward.		Implemented
13. Performance data is obtained and reviewed to ensure managers can monitor contractors' performance against targets and contract terms and conditions. Where targets are not being met the contractor should submit proposals for improving performance. Additionally, officers should be aware of any financial implications of contractors not meeting their contractual agreements, to ensure that these can be enforced if required.	High	The planned structure for the service includes provision to enable this process. New contracts also support this approach. The audit plan for 2024/25 includes a housing contract management audit, to be carried out later in the year which will test and validate this approach.	Head of Housing	Q4 2024/25

HOUSING REPAIRS



Areas of positive assurance identified during the audit:

- Officers have been trained in the procedures and processes appropriate to their areas of work.
- Pre and post inspections are being completed promptly on all empty homes and documentation is being retained.
- Contractors' schedules of rates are up to date on the housing management system (QL).
- Complaints were dealt with in accordance with the corporate complaint policy.

The main areas identified for improvement are:

- Regular review of policies and procedures.
- Prioritisation is aligned with sector standards and service level agreements, and manual intervention on the system is removed.
- Regular monitoring of orders and variations to ensure work is progressed timely and orders closed appropriately.
- A process needs implementing to capture, document and monitor pre-inspections, post inspections and specialist surveys.
- A consistent approach is required for the processing of consolidated invoices which ensures all appropriate checks are made prior to payment and invoices are processed in a timely manner.
- Contracts need to be relevantly managed and monitored.
- A process needs to be put in place to ensure recharges are identified, accurately cost, document and recovered.
- Adequate insurance arrangements need putting in place for all van stock.
- A review of Service performance monitoring and indicators to ensure the authority is fulfilling its statutory duties as a landlord.

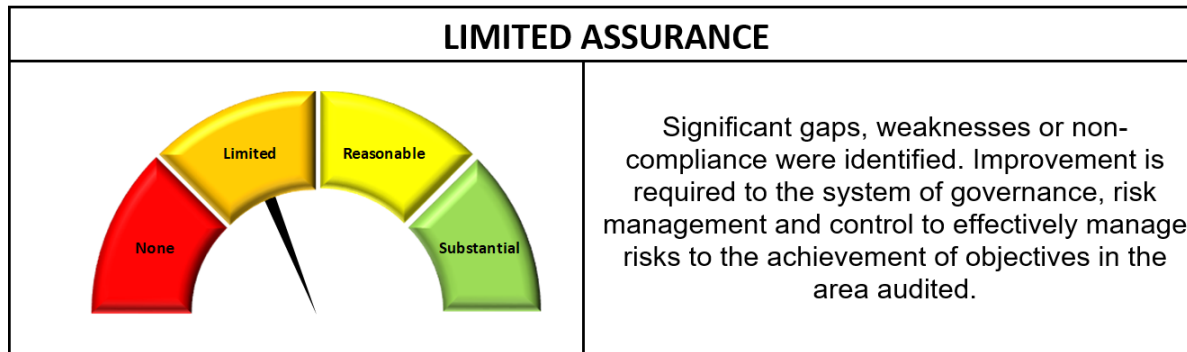
Recommendation	Priority	Response/Agreed Action	Officer Responsible	Implementation Date
1. The Council's website is updated with the new policies ensuring up to date information is available to the public.	Low	These have been updated on the website.		Implemented
2. The tenants handbook is revised to reflect any changes in policy.	Low	This will be updated in line with the latest policy changes. However, this requires tenant involvement in the process. This work is currently being programmed.	Housing Management Team Manager	December 2024
3. All key procedures are reviewed and updated to reflect current working practices, ensuring it is clear who the responsible officer is, they reflect current working practices and comply with legislative requirements.	Low	Work has commenced on reviewing the procedures. Since the Audit, a restructure has been actioned which changes the responsibilities between teams. Once this is completed the end-to-end process will be updated. Details given to operatives has already been operationally updated.	Head of Housing	April 2025
4. Following the mobilisation of the contractor, system parameters are updated to correspond with any changes.	High	The updated policy was agreed by Cabinet in April 2024. The implementation of the updated policy will be brought forward once the 'catch up' repairs contract is fully operational.	Head of Housing	December 2024
5. The system parameters are amended to prevent officers changing target completion dates.	Medium	Agree in principle, however this is currently not possible and therefore exception reporting and monitoring through 'touch point' software has been introduced to ensure that the relevant control issues identified are being appropriately managed.		Implemented
6. Investigate the possibility of setting parameters within the housing management system so that through the selection of schedule of rate and trade codes the system determines the priority for the order to remove the need for officers raising orders to have to make decision, ensuring that prioritisation of orders is consistent.	Medium	Agreed in principle, this will be reviewed once a full complement of Senior Management Team is in place. Currently being managed through exception reporting.	Head of Housing	September 2025
7. Regular monitoring of orders, follow on work, and variations is undertaken to ensure orders are issued, progressed, follow on work scheduled, variations promptly approved, and orders completed.	High	An extensive amount of work has been done since the audit and all numbers have been reduced. Regular monitoring has now been introduced and Audit is requested to re visit this recommendation with the service in Q4 to provide assurance on this identified control weakness.	Head of Housing	Q4 2024/25

8. A review is undertaken to ensure all contractors are assigned SOR books.	Medium	The Service is in the process of major re-contracting of all contracts across the service. As part of this process SOR pre contracts will be enacted within the system.	Head of Housing	April 2025
9. Pre inspection and post inspections showing on the housing management system as outstanding should be reviewed to confirm their status.	Medium	A management decision will be made on closing inspections over a set time. Inspections going forward will be undertaken on a percentage of work – urgent, Housing Health & Safety Rating System (HHSRS) and high value works.	Head of Housing	December 2024
10. A process is put in place to capture, document and monitor pre-inspection, post inspection and specialist surveys to ensure appropriate work is undertaken and tenants' homes meet the standard required.	High	These processes will be put in place once a substantive management and operational team is in place within the service, and contractors are embedded.	Head of Housing	April 2025
11. Management should consider the use of e-forms or appropriate software to capture and store inspections and review the system parameters for the automatic selection of properties to be post inspected to ensure they are appropriate.	Medium	Agreed – the Service is enacting an e-form process as described.	Head of Housing	April 2025
12. The signing off of the work completed by the QS is documented on the order within the housing management system (QL).	Medium	These processes will be put in place once a substantive management and operational team is in place within the service, and contractors are embedded.	Head of Housing	April 2025
13. Orders are changed to a history status when the contractor has been paid to prevent duplicate payment and ensure QL is accurate and up to date.	Medium	Work is ongoing with finance on overall process review. As part of the procedures work (elsewhere covered on this audit) it will also address this. The Service is seeking to automate this process between the finance and Housing systems. Historic jobs will be closed.	Head of Housing	April 2025
14. A payment mechanism is agreed with contractors and is put in place for the processing of consolidated invoices, ensuring a timely, consistent approach.	Medium	The service is re-contracting all major suppliers. During this process the management of batch payments and invoicing has been addressed. The audit plan for 2024/25 includes a housing contract management audit, to be carried out later in the year which will test and validate this approach.	Head of Housing	Q4 2024/25
15. Payment Certificates are signed by the Contract Administrator before payment is made.	High	The planned structure for the service includes provision to enable this process. New contracts also support this approach.	Head of Housing	Q4 2024/25

		The audit plan for 2024/25 includes a housing contract management audit, to be carried out later in the year which will test and validate this approach.		
16. All invoicing documentation is stored on the housing shared drive and documents are filed in a clear consistent manner, to ensure that key documents are easily identified.	Medium	This has been fully resolved and the approach of personal drive use has ceased.		Implemented
17. Officers are given training on the use of unauthorised software and secure storage of documentation to ensure data protection is not breached.	High	This approach has been ceased and an IT action has blocked any further use of this.		Implemented
18. Each contract is assigned to a specific contract officer who will be responsible for managing and monitoring the relevant contracts. This will ensure that any breaches are identified and rectified promptly.	High	The planned structure for the service includes provision to enable this process. New contracts also support this approach. The audit plan for 2024/25 includes a housing contract management audit, to be carried out later in the year which will test and validate this approach.	Head of Housing	Q4 2024/25
19. Performance monitoring data is obtained from the contactors for review to ensure contract conditions are being met. 8	Medium	The planned structure for the service includes provision to enable this process. New contracts also support this approach. The audit plan for 2024/25 includes a housing contract management audit, to be carried out later in the year which will test and validate this approach.	Head of Housing	Q4 2024/25
20. Outstanding recharges debt is regularly monitored and relevantly reported.	Medium	A review of the process of managing and reporting rent accounts is in progress. This will be addressed as part of this review.	Housing Strategy and Systems Team Manager	March 2025
21. Management explore using the housing management system (QL) to identify and create recharge rent debit removing the need for internal recharge forms.	Medium	A review of the process of managing and reporting rent accounts is in progress. This will be addressed as part of this review.	Housing Strategy and Systems Team Manager	March 2025
22. Processes are reviewed, and appropriate controls are put in place to identify, accurately cost, document, and recover recharges to tenants. In conjunction with the above, management consider introducing a minimum recharge limit and explore the	Medium	In April 24, a new policy regarding repairs approaches was adopted. This includes an improved management of recharges for works related to repairs. Other aspects of this recommendation will be addressed via the review of our reporting and management of rent accounts.	Housing Strategy and Systems Team Manager	March 2025

capabilities of the Aareon Versa Mobile System to streamline the process.				
23. The Compensation Policy is reviewed, distributed to the relevant officers and training on the process given where appropriate.	Medium	The Compensation Policy was reviewed and agreed by Cabinet in April 24. Distribution has taken place and training is planned to be provided where appropriate to the limited number of staff involved in the process.		Implemented
24. Procedures are put in place to ensure compensation payments are appropriately authorised.	Medium	Compensation approaches and authorisation levels are set out in the revised Compensation Policy adopted by Cabinet in April 24. Compensation via the complaints process is all either authorised at Director or CEO level. Others are approved in line with the policy.		Implemented
25. Appropriate insurance is arranged for stock held on vehicles.	Medium	There is no insurance provision through Zurich and there never has been. Due to the value, the Council would not seek to transfer this risk and instead provide self-insurance and any losses would be covered by the Housing Revenue Account.		Implemented
26. A review of performance monitoring and indicators is undertaken to ensure that the organisation is capturing sufficient and accurate information and that what is being produced is measurable, objective focussed and meaningful, and is reported and reviewed on a regular basis.	Medium	Monitoring of the housing service is undertaken by the approach adopted by Council in Q3 2023 when it approved the Council Delivery Plan (CDP). This includes a specific target in the CDP, several in the Business Plan (adopted Q4 2023), and the Housing Service plan adopted in June 24 and endorsed by the cross-party Housing Improvement Board. These are all following the corporate adopted monitoring approach. In addition, data monitoring of key indicators is undertaken across the service on a monthly basis. Monitoring of the national Tenant Satisfaction Measures are also undertaken and published to the regulator and on the Council's website. Pay Performance Agreement (PPA) monitoring has been suspended whilst this is being renegotiating. Staff pay has not been impacted whilst negotiations continue.		Implemented

HOUSING ASBESTOS MANAGEMENT



Areas of positive assurance identified during the audit:

- There is an approved Asbestos Management Policy, dated October 2023.
- Roles and responsibilities in relation to Asbestos Management are documented in the Asbestos Management Policy.

27

The main areas identified for improvement are:

- There being a complete set of procedures relating to asbestos management in Housing.
- Having an approved Asbestos Management Plan, as referred to in the Asbestos Management Policy, which is regularly reviewed and updated.
- Agreeing the format of the Asbestos Register and assignment of responsibility to ensure the register is kept up to date.
- Maintaining records to enable monitoring of results of asbestos surveys to ensure action is taken as required.
- Carrying out assessments to confirm compliance with the Council's statutory duties relating to asbestos.
- Uploading of asbestos surveys and other any relevant certificates / documents to the Housing System (QL and MRI).
- Having effective contract management in place, with named contract managers, regular minuted contractor meetings, establishing and monitoring of key performance indicators, provision of financial information relating to the contract etc.
- Ensuring that officers have received the required level of asbestos management training for their role.

Recommendation	Priority	Response/Agreed Action	Officer Responsible	Implementation Date
1.An Asbestos Management Plan, as referred to in the Asbestos Management Policy, should be completed, approved, made available to staff, and appropriately reviewed and managed.	High	The Asset Team Leader has been working on the Asbestos Management Plan with The Health and Safety Officer, the final draft review is pending completion to submit to Corporate Leadership Team (CLT) for approval and corporate distribution.	H&S Officer / Responsible Person	December 2024
2.The Asbestos Procedures and Guidance document should be reviewed and updated to ensure that it captures all key procedures and processes relating to asbestos management.	High	A revision will be completed, tie in with issue of AMP.	Asset Team Leader/ Head of Housing / External Consultants	December 2024
3.The Council should conduct an assessment to identify all areas of non-compliance of statutory duties in relation to Asbestos Management. Following this an action plan should be put in place to ensure that the non-compliance is addressed. Assessments should then be scheduled at regular intervals to ensure ongoing compliance.	High	<p>The Asset Management team holds reports to cover compliance of over 95% of the domestic stock and 100% of communal to comply with CAR2012.</p> <p>The Asset Management team has assessed where non-compliance is occurring and, in the majority, falls down to lack of resources that are managed or influenced by the following –</p> <ul style="list-style-type: none"> • Two managers absent on long term sick leave. • Failing to recruit to three team crucial posts. • One post being carried out by an unqualified member of staff. <p>Due to the lack of resources, the data received day to day, operational admin and data management is not being completed to a sufficient standard. Minimal admin is undertaken, and other staff resources are being utilised to pick up the short fall. Quality assurance is at risk due to insufficient administration of the asbestos data and as a consequence puts operatives, contractors, staff and other end users at risk.</p> <p>Failure to manage properly exposes NWLDC to prosecution from the Regulator, HSE and leading to unlimited fines.</p> <p>The service is continually trying to actively recruit, however, to reduce/ remove the risks associated with the control issues identified, the Housing Asset Management</p>	Head of Housing	November 2024

		team is currently reviewing options available to them which include outsourcing the control and quality assurance of the asbestos data that is relied on.		
5.Asbestos surveys should be uploaded to QL / MRI within a reasonable period of time following receipt of the survey.	High	This is a known issue that can only be resolved by adequate resourcing and addressing the issues detailed in the response to recommendation 3 above. The Tersus portal will be used initially to reduce the risks.	Compliance Team Leader – when appointed	November 2024
6.There should be a central record containing details of asbestos surveys, the results of the surveys and any action to be taken. The record should be used to enable effective monitoring of actions required. Responsibility for ensuring the record is maintained and actions completed should be assigned.	High	Whilst there are various locations for data held, Asset Management have been working on reducing data suppositories to MRI, QL or the contractor portal. A central record is being developed to streamline how these are maintained so there is adequate visibility to all users of the data held. It is to be noted again that this is only feasible with the resourcing issues identified in the response section in recommendation 3. being addressed.	Compliance Team Leader – when appointed	March 2025
7.The contract with Tersus Consultancy should be finalised and copies provided to relevant staff.	High	Contracts were prepared earlier in the year and were delayed due to resourcing issues. The contract is being chased by legal to complete its final processes.	Asset Manager / Legal	August 2024
8. All contracts should have a named contract manager and formal contract management arrangements should be put in place.	High	This is a known process within Asset Management. Actioning this process and formally following through with normal contract administration is not possible with the current lack of resources to manage individual contracts. The planned structure for the service includes provision to enable this process. New contracts also support this approach. The audit plan for 2024/25 includes a housing contract management audit, to be carried out later in the year which will test and validate this approach.	Head of Housing	Q4 2024/25
9.Key performance indicators (KPI's) and the frequency to which they should be reported to management should be agreed with asbestos contractors. Service Plan KPI's should be a standard agenda item in any contract management meetings.	High	This is a known process within Asset Management and when administrating contracts. The delays in executing and mobilising the contract have set back formalising these arrangements. Adequate resourcing is also essential in capturing this data set. The new suite of KPI's will be discussed at contract management meetings now the new contract is nearly in place.	Head of Housing	Q4 2024/25

<p>10. Advice should be sought from the Procurement Team/ Director of Resources regarding overspends against contract values and any action to be taken.</p>	High	<p>Central finance systems are difficult to extract and interrogate financial expenditure and budgets to effectively manage contracts.</p> <p>Training sessions have been identified and are being rolled out.</p> <p>Asbestos removal is contractually administered by the Repairs Team Manager – which has been vacant for a considerable time.</p>	<p>Asset Team Manager / Asset Manager/ Commercial services Team Manager / Repairs Team Manager / Finance</p>	December 2024
<p>11. Following receipt of the Schedule of Rates from Tersus Consultancy, invoices from the start of the contract should be reviewed to confirm that the Council has been correctly invoiced.</p>	High	<p>This is a known process within Asset Management and when administrating contracts. The delays in executing and mobilising the contract have set back formalising these arrangements.</p> <p>Adequate resourcing is also essential in capturing this data set.</p> <p>The planned structure for the service includes provision to enable this process.</p> <p>This issue may have been due to the agency contractor not having site of the framework rates.</p> <p>A review will be carried out</p>	Head of Housing	March 2025
<p>12. For each of the asbestos contracts financial information should be produced and presented to management for both monitoring and discussion at contract management meetings.</p>	High	<p>This is a known process within Asset Management and when administrating contracts. The delays in executing and mobilising the contract have set back formalising these arrangements.</p> <p>Adequate resourcing is also essential in capturing this data set.</p> <p>Agree in principal but, until Unit 4 is fully operational this will not be possible to implement.</p>	Head of Housing	March 2025
<p>13. The Council should ensure that all relevant staff have received / undertaken the level of training in Asbestos Management as required by either their job role or their assigned role within the Asbestos Management Policy.</p>	Medium	<p>Whilst all operational staff have the minimum Asbestos Awareness training others at team leader, supervisor and management have received Duty to Manage training.</p> <p>Whilst this is recognised as a minimum requirement, it has been identified that team managers should receive P405 training to mitigate risk at a higher level and to cover duty holder requirements in the absence of other Responsible Persons.</p>	Head of Housing and Strategic Director of Communities	<p>September 2024</p> <p>Training dates will be advised following the review.</p>

		HR, in conjunction with managers/ Heads of Service, will be requested to carry out a review of which officers require which level of training across the authority. Following this, training will be arranged.		
--	--	---	--	--

EXTENDED RECOMMENDATIONS

Audit Year	Audit	Recommendation	Priority	Response/ Agreed Action	Responsible Officer	CLT	Original Due Date	1st Follow up comments	Extension Date	Second Follow up comments	Extension Date	Further Management update	Further 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	Jul-23: Partially completed in that some policies are now in place.	Dec-23	Dec-23: There are policies in place now for Legionella, Asbestos, Fire Risk Management and General Health and Safety. Nothing confirmed for Electrical Management Policy	Oct-24
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	Jul-23 – Good progress is being made but consultants still engaged.	Dec-23	Dec-23 Contractor performance is currently being monitored via the Statutory Duty Group. Further improvements are expected to be delivered by the council adopting a digital Asset Management System to work alongside the Asset Management Toolkit currently being prepared. Work to identify Asset Management Systems is with implementation and onboarding likely to take 6 months.	Oct-24
2021/22	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.	Strategic Director	Strategic Director	Mar-23	Extended to align with other recommendations	Jul-23	Jul-23 – Good progress is being made but consultants still engaged.	Dec-23	Dec-23 As detailed above, the adoption of a new system will assist with meeting legislative compliance. Following this full consideration will be given to adopting a corporate landlord model.	Oct-24 for system implementation Dec-24 for decision on the adoption of a corporate landlord model.

				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.									
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	Jul-23 – Good progress is being made but consultants still engaged.	Dec-23	As per recommendation 2	Oct-24
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	Jul-23 – Good progress is being made but consultants still engaged.	Dec-23	The digital Asset Management System will automatically schedule inspections at the required frequency. It is expected that a decision on which Asset Management system is to be adopted will be taken by 31/3/2023 with implementation and onboarding likely to take 6 months thereafter.	Oct-24
73													
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	Director of Resources	Director of Resources	Dec-22	Recommendation extended due to corporate review	Sep-23	As per recommendation 1	Mar-24	Mar-24: The upcoming training sessions, scheduled for later this year, will be particularly beneficial once the new templates and guidance materials are available. Paul Kaerger, with his expertise from PKMS, will be a good choice to lead these sessions, bringing valuable insights and experience to the training program. June-24: Project management training is	April-24 Oct-24

													scheduled for September 2024, with a neighbouring authority. Additionally, an e-learning module will be developed later this year.	
2022/23	Rent Accounting and Arrears	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	Director of Communities	Aug-23	Aug 23 – No response	Sept 23	Sept 23 - Issues regarding UNIT4 - meeting with Finance planned for w/c 11.9.23. Will require an extension to the implementation date.	Oct 23	Nov-23 Further extension requested.	Mar-24 Sept-24	
2022/23	Payroll	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 and Head of HR and Organisational Development	Director of Resources/ Head of HR & OD	April-24	Not implemented due to resourcing issues/ staff leaving. Will further discuss with Director of Finance and Head of Finance.	July-24					
74														
2022/23	Payroll	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.	Head of HR and Organisational Development	Dec-23	Dec 23 – Not implemented due to resourcing issues/ staff leaving. Will further discuss with Director of Finance and Head of Finance.	July 24					
2022/23	Payroll	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.	Head of HR and Organisational Development	Dec-23	Dec 23 – Not implemented due to resourcing issues/ staff leaving. Will further discuss with Director of Finance and Head of Finance.	July 24					
2022/23	Payroll	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	Director of Resources	Dec-23	Dec-23 Testing to be undertaken in January with changes to NI and again Feb/ March.	July-24					
2022/23	Payroll	5. On, at least, an annual basis an establishment report from iTrent should be	High	Agree – report to be obtained from iTrent and issued on an annual basis.	Head of HR and Organisational Development.	Head of HR and Organisational	Mar-24	Extended as requested.	July-24					

		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.				Development							
2022/23	Payroll	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	Director of Resources / Head of HR and Organisational Development	Dec-23	Dec 23 – Not implemented due to resourcing issues/ staff leaving. Will further discuss with Director of Finance and Head of Finance.	July 24				
2022/23	Payroll	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	Head of HR and Organisational Development	Dec-23	Dec 23 – Not implemented due to resourcing issues/ staff leaving. Will further discuss with Director of Finance and Head of Finance.	July 24				
75													
2022/23	Payroll	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	Head of HR and Organisational Development	Dec-23	Dec 23 – Not implemented due to resourcing issues/ staff leaving. Will further discuss with Director of Finance and Head of Finance.	July 24				
2022/23	Payroll	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	Head of HR and Organisational Development	Dec-23	Dec 23 – Not implemented due to resourcing issues/ staff leaving. Will further discuss with Director of Finance and Head of Finance.	July 24				
2022/23	ASB	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.	Head of Housing	Mar-24	March 23: New set of indicators within the policy. Extension to ensure that these are fully embedded and reported following the approval of the Policy at Cabinet	July 24				

2022/23	ASB	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 response 17.7.23: a new suite of indicators is now being captured in line with the Tenant satisfaction measures outlined by the Social Housing regulator.	Housing Management Team Manager.	Head of Housing	Mar-24	March 23: New set of indicators within the policy. Extension to ensure that these are fully embedded and reported following the approval of the Policy at Cabinet	July 24				
2023/24	Safeguarding	7.The updated DBS Policy should be made available to staff on SharePoint. The out-of-date DBS Policy should be removed from SharePoint to avoid confusion.	High	Agreed	Head of HR and Organisational Development	Chief Executive	May-24	June 24 - The revised policy will be considered by CLT in early August 2024 and sharepoint will then be updated accordingly.	Oct-24				
2023/24	Safeguarding	8.Staff required to have DBS checks should be made aware of the requirement to have annual rechecks, the results of which should be provided to and recorded by HR. Consideration should be given to including this as an item within the annual Individual Development Review (IDR) to ensure that it is not overlooked. Consideration should be given to including this as an item within the annual Individual Development Review (IDR) to ensure that it is not overlooked.	High	Agreed – however the policy is to be changed and the requirement will be for DBS rechecks to be completed every three years.	Head of HR and Organisational Development	Chief Executive	May-24	June 24 - An updated list of posts requiring checks is being circulated to managers and when the revised policy has been agreed by CLT all staff checks will be renewed. The results of the checks will then be recorded on I-Trent and reminders will then be auto-generated to managers and employees at the 3 year anniversary.	Oct-24				
2023/24	Procurement and Contracts	3.The contract register should be reviewed and updated on a regular basis to ensure compliance with the Local Government Transparency Code. Responsibility for updating the contracts register should be relevantly assigned.	High	Agreed. This is currently in train. If the full information is not available, will publish and add full detail at a later date.	Procurement Officer	Director of Resources	Jun-24	June 24 – The data continues to be compiled. It is intended that the register will be published on the Council's website by the end of July.	Aug-24				

2022/23	Rent Accounting and Arrears	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.	Director of Communities	Dec-23	Dec 23 – This will be picked up following the policy audit report being presented to CLT.	Jun-24	June 24 – To be addressed through the ongoing policy review process and through the specific Rent Accounting Audit recently completed.	Mar-25		
2022/23	Rent Accounting and Arrears	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	Director of Communities	Jun-24	June 24 – To be addressed via the Head of Housing working with the Head of Finance and the Housing Systems and Strategy Team Leader.	Dec-24				

2024/25 INTERNAL AUDIT PERFORMANCE

Performance Measure	Position as at 30.06.2024	Comments
Achievement of the Internal Audit Plan	0%	This is due to the delays in completing the 2023/24 audit plan.
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 received during 2023/24
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.

Likely to contain exempt information under paragraph(s) 3 of Part 1 of Schedule 12A of the Local Government Act 1972.

Document is Restricted

This page is intentionally left blank

NORTH WEST LEICESTERSHIRE DISTRICT COUNCIL

AUDIT AND GOVERNANCE COMMITTEE – WEDNESDAY, 7
AUGUST 2024

Title of Report	REVIEW OF CORPORATE GOVERNANCE POLICIES	
Presented by	Paul Stone Strategic Director of Resources	
Background Papers	None	Public Report: Yes
Financial Implications	There are no financial implications to be considered.	
	Signed off by the Section 151 Officer: Yes	
Legal Implications	The policies are reviewed annually to ensure any updates in the law are noted so that the Council acts in accordance with the law.	
	Signed off by the Monitoring Officer: Yes	
Staffing and Corporate Implications	The suite of Corporate Governance Policies is regularly reviewed to ensure the Council operates effectively, in line with the appropriate standards.	
	Signed off by the Head of Paid Service: Yes	
Purpose of Report	To receive the Committee's comments on the Council's annual review of the Corporate 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 24 SEPTEMBER 2024.	

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 the 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	2023

Anti-Money Laundering Policy	2023
Confidential Reporting (Whistleblowing) Policy	2023
Risk Management Policy	2023
RIPA Policy	2023
Local Code of Corporate Governance	2023
Data Protection Policy	2023
Information Governance Framework	N/a
Information Security Policy	2023 (formerly the ICT and Cyber Security Policy)
Information Rights Policy	2023 (formerly Information Management Policy)
Records Management Policy	2023 (formerly Information Management Policy)

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 on 24 September 2024.

2.0 POLICY REVIEW

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

As part of the review process, all policies now incorporate a standardised format which sets out key policy details at the start of the document and ensures that completion of an Equality Impact Assessment (EIA) is documented at the end of each policy.

There are some policies that authors have not been able to complete the EIA form for yet. Those policies are the Anti-Fraud and Corruption Policy, the Anti-Money Laundering Policy, the Confidential Reporting (Whistleblowing) Policy and the Local Code of Corporate Governance Policy. Policy authors will ensure that the EIA form is completed in respect of each of these policies prior to them being taken to Cabinet, however, authors have indicated that they do not consider the policies to have a prejudicial impact on equalities and therefore it is unlikely that a full EIA form will be required.

The main changes to each policy are summarised below.

Anti-Fraud and Corruption Policy

There have been no changes in legislation that affect this policy since the previous review. Therefore, only minor amendments have been made including updates to names referenced within the policy.

Anti-Money Laundering Policy

There have been no changes in legislation that affect this policy since the previous review. Therefore, only minor amendments have been made including updates to names, contact details and dates referenced within the policy.

Confidential Reporting (Whistleblowing Policy)

There have been no changes in legislation that affect this policy since the previous review. Therefore, only minor amendments have been made including updates to names, contact details and the Council's address. References within the policy to the external audit firm

have also been updated as the Council's external auditor has changed from Mazars to Azets.

Risk Management Policy

The policy has been amended to confirm that the Audit and Governance Committee is responsible for reviewing the Corporate Risk Register, as per the Council's Constitution. Further clarity around identifying risks has also been inserted in the appendix.

Minor amendments including renames of groups referenced within the policy, insertion of the role of Members to the appendix and formatting revisions have also been made.

A graphic has also been inserted at Section 4 'Risk Management Policy' to illustrate the objectives of the Council's Risk Management Policy. This involves the process of identifying, assessing, managing and controlling and reviewing and reporting risks.

RIPA Policy

There have been no changes in legislation that affect this policy since the previous review. Therefore, only minor amendments have been made including updating the edition date of the Home Office Code of Practice to reflect the latest publication.

Local Code of Corporate Governance

There have been no changes in legislation that affect this policy since the previous review. Therefore, only minor amendments have been made to the formatting of the document.

Information Governance Framework

The Council has been undertaking a review of information governance, as reported to the Audit and Governance Committee through the Senior Information Risk Officer's Annual Report on 24 April 2024. As part of that review, it was identified that it would be helpful to bring together all of the Information Governance Policies into one single framework.

The Information Governance Framework is, therefore, a new document that sets out the Council's approach to information governance, including four key principles that underpin good information governance – information rights, records management, data protection and information security. To underpin the importance of each of these principles, there is a policy for each that sets out the Council's commitments in each of those areas. Supporting these policies are internal standards, procedures and guidance that officers will keep updated to implement the requirements of the policies.

All the policies have been updated into a streamline format with the aim of making them easy to understand and follow. The new framework is, therefore, a consolidation of existing policies but in a new format and layout, with appropriate cross-referencing and connections between all four policies.

This will be the format of the Information Governance policies going forward and in future years, the Information Governance Framework and the four policies that accompany it will be reviewed as a collective and brought back to the Audit and Governance Committee each year as part of the annual Corporate Governance Policies Review.

Policies and other considerations, as appropriate	
Council Priorities:	A Well-Run Council.
Policy Considerations:	As detailed within the 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 any negative economic impacts.
Environment, Climate Change and Zero Carbon	N/a
Consultation/Community/Tenant Engagement:	N/a
Risks:	As part of its Corporate Governance arrangements, the Council must ensure that risk management is considered and satisfactorily covered in any report put before elected Members for a decision or action. The purpose of this report is to set out the review undertaken by Corporate Governance Policy authors and detail the changes made. As part of this, the Risk Management Policy is reviewed annually.
Officer Contact	Paul Stone Strategic Director of Resources Paul.stone@nwleicestershire.gov.uk



ANTI-FRAUD AND CORRUPTION POLICY

Item	Details
Reference:	Internal Audit – 1 – AF&CP
Status:	Draft
Originator:	Kerry Beavis
Owner:	Kerry Beavis
Version No:	2.7
Date:	[To be inserted once approved and published]

Key policy details

Approvals

Item	Date of Approval	Version No.
Consulted with	N/A	N/A
Reviewed by Audit and Governance Committee	7 August 2024	2.7
Approved by Cabinet	24 September 2024	2.7

The policy owner has the authority to make the following minor changes without approval

N/A

Policy Location

This policy can be found on NWLDC's website and the SharePoint page.

Revision history

Version Control	Revision Date	Summary of Changes
2.1	September 2015	
2.2	October 2019	
2.3	May 2020	
2.4	June 2021	
2.5	June 2022	
2.6	June 2023	Minor amendments – name and job title changes.
2.7	July 2024	Minor amendments – name change

Policy Review Plans

This policy is subject to a scheduled review annually or earlier if there is a change in legislation or local policy that requires it.

Distribution

Title	Date of Issue
Audit & Governance Committee	7 August 2024
Cabinet	24 September 2024
Available on NWL website	[To be confirmed]

	Contents
1.	Introduction
2.	Scope
3.	Definitions
4.	Culture
5.	Responsibilities
6.	Prevention and deterrence
7.	Detection and investigation
8.	Raising concerns
Appendix A	

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 practice 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 The Council has determined that the culture and tone of the organisation will be one of honesty and opposition to fraud and corruption. Malpractice or wrongdoing in the provision of our services will not be tolerated and the Council is 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 is 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: paul.stone@nwleicestershire.gov.uk
Telephone 01530 454495
- Audit Manager: kerry.beavis@nwleicestershire.gov.uk
Telephone 01530 454728

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)

Equality Analysis

Completion of Equality Impact Assessment (EIA) Form

Has an EIA form been completed as part of creating / reviewing / amending this policy?	Please tick: Yes <input type="checkbox"/> No <input type="checkbox"/>
If yes, where can a copy of the EIA form be found?	
If no, please confirm why an EIA was not required?	

This page is intentionally left blank



ANTI-MONEY LAUNDERING POLICY

Item	Details
Reference:	Internal Audit – 2 - AML
Status:	Draft
Originator:	Kerry Beavis
Owner:	Kerry Beavis
Version No:	2.6
Date:	[To be inserted once approved and published]

Key policy details

Approvals

Item	Date of Approval	Version No.
Consulted with	N/A	
Reviewed by Audit and Governance Committee	7 August 2024	2.6
Approved by Cabinet	24 September 2024	2.6

The policy owner has the authority to make the following minor changes without approval

N/A

Policy Location

This policy can be found on NWLDC's website and on the SharePoint page.

Revision history

Version Control	Revision Date	Summary of Changes
2.1	September 2015	
2.2	May 2020	
2.3	June 2021	
2.4	June 2022	
2.5	June 2023	Minor amendments - name changes.
2.6	July 2024	Minor amendments - name changes.

Policy Review Plans

This policy is subject to a scheduled review once annually or earlier if there is a change in legislation or local policy that requires it.

Distribution

Title	Date of Issue
Audit & Governance Committee	7 August 2024
Cabinet	24 September 2024
NWL Website	[To be confirmed]

	Contents
1.	Introduction
2.	Scope of the policy
3.	Definition of money laundering
4.	Requirements of the money laundering legislation
5.	The money laundering reporting officer (MLRO)
6.	Client identification procedures
7.	Reporting procedure for suspicions of money laundering
8.	Consideration of the disclosure by the money laundering reporting officer
9.	Training

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 2023, 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 during 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 moneylaundering 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 on 01530 454495 or at paul.stone@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.

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.

- 7.3 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.
- 7.4 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'.
- 7.5 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.

Equality Analysis

Completion of Equality Impact Assessment (EIA) Form

Has an EIA form been completed as part of creating / reviewing / amending this policy?	Please tick: Yes <input type="checkbox"/> No <input type="checkbox"/>
If yes, where can a copy of the EIA form be found?	
If no, please confirm why an EIA was not required?	

This page is intentionally left blank



CONFIDENTIAL REPORTING (WHISTLEBLOWING) POLICY

Item	Details
Reference:	Internal Audit – 3 - CR
Status:	Draft
Originator:	Kerry Beavis
Owner:	Kerry Beavis
Version No:	2.5
Date:	[To be inserted once approved and published]

Key policy details

Approvals

Item	Date of Approval	Version No.
Consulted with	N/A	
Reviewed by Audit and Governance Committee	7 August 2024	2.5
Approved by Cabinet	24 September 2024	2.5

The policy owner has the authority to make the following minor changes without approval

N/A

Policy Location

This policy can be found on NWLDC's website and on the Sharepoint page.

Revision history

Version Control	Revision Date	Summary of Changes
2.1	May 2020	
2.2	June 2021	
2.3	June 2022	
2.4	June 2023	
2.5	July 2024	Minor amendments, including name changes and updates to the external audit firm and the Council's address.

Policy Review Plans

This policy is subject to a scheduled review annually or earlier if there is a change in legislation or local policy that requires it.

Distribution

Title	Date of Issue	Version No.
Audit & Governance Committee	7 August 2024	2.5
Cabinet	24 September 2024	2.5
Available on NWL website	[To be confirmed]	2.5

	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 workers to feel confident in raising concerns that are in the public interest and to question and act upon concerns;
- provide avenues for workers to raise those concerns and receive feedback on any action taken;
- ensure that workers receive a response to their concerns and that they are aware of how to pursue matters if they are not satisfied;
- reassure workers that they will be protected from the risk of reprisals or victimisation if they have a reasonable belief that they 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. Workers are legally entitled to protection from unfair treatment if:

(a) they honestly think what they are reporting is true,

(b) they believe that they are telling the right person,

(c) they believe that raising concerns is in the public interest.

Put simply, if an individual is acting in good faith when raising any concerns, they should have nothing to fear because they will be doing their duty to their employer, and/or the Council and those for whom the Council provides a service. In the event that the concerns raised are substantiated, they 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 the identity of the person making the complaint where they so wish. The Council cannot ensure confidentiality where the individual has themselves 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 the individual's identity. The individual will, however, still be entitled to the same protection against harassment, victimisation, and other pressures as if their identity remained confidential.

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

4.4 It should be noted that, whilst every effort will be made to protect an individual's identity, the Council may, at an appropriate time ask them to come forward as a witness. If they do become a witness in any case, they will be entitled to the same protection against harassment, victimisation, and other pressures that they 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 them 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
- Section 151 Officer:
paul.stone@nwleicestershire.gov.uk
Telephone 01530 454495
- 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:

Whitwick Business Centre
Whitwick Business Park
Stenson Road
Coalville
Leicestershire
LE67
3FJ

Clearly mark the envelope "Confidential".

Alternatively, any concerns can be raised with North West Leicestershire District Council's external auditors:

Azets
6th Floor
Bank House
Cherry Street
Birmingham
B2 5AL

- 7.3 Concerns can be raised in the following ways –

- A written report using the following format:
 - the background and history of the concern (giving relevant dates);
 - the reason why the situation is of particular concern.

- A verbal report of any concerns identified by contacting one of the officers named at paragraph 7.1 above to arrange a mutually convenient appointment. When arranging an appointment, it would be helpful to refer to raising a matter under the Confidential Reporting Policy.
 - When making a verbal report set out the facts using the same format identified at paragraph 7.3 above.

- 7.5 The earlier concerns are raised the easier it is for the Council to investigate and take any relevant action.

- 7.7 When raising a concern, the individual will not be expected to prove beyond doubt the truth of an allegation but will need to demonstrate to the person contacted that there are reasonable grounds for concern.

- 7.8 An individual may wish to consider discussing their concern with a colleague or trade union representative first and may find it easier to raise the matter if two (or more) share any concerns.

- 7.9 The individual wishing to raise a concern may invite a trade union representative, professional association representative or a member of staff to be present during any meetings or interviews in connection with the concerns raised, any meetings may be arranged off-site if appropriate.
- 7.10 If an individual feels unable to raise concerns directly with the Council, they should report the matter to a “prescribed person”. This will ensure that their 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 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 the individual raising the concern in order to gain further information. Do not forget that testing out 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 the individual raising the concern:
- acknowledging that the concern has been received,
 - indicating how the Council propose to deal with the matter,
 - give an estimate of how long it will take to provide a final response,

- advising whether any initial enquiries have been made,
- providing information on staff support mechanisms, and
- advising whether further investigations will take place and if not, why not.

8.7 The amount of contact between the officers considering the issues and the individual 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 the individual.

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

8.9 The Council accepts that an individual needs to be assured that the matter has been properly addressed. Thus, subject to legal constraints, we will inform the individual 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 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 individuals with an avenue within the Council to raise concerns. The Council hopes the individual will be satisfied with any action taken. If not, and they feel it is right to take the matter outside the Council, the following are possible contact points:

- one of the “prescribed persons”
- trade union
- 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 the matter is taken outside the Council, the individual should ensure that they do not disclose confidential information. Check with one of the Council’s nominated contact points about that (see 7.1).

Equality Analysis

Completion of Equality Impact Assessment (EIA) Form

Has an EIA form been completed as part of creating / reviewing / amending this policy?	Please tick: Yes <input type="checkbox"/> No <input type="checkbox"/>
If yes, where can a copy of the EIA form be found?	
If no, please confirm why an EIA was not required?	

This page is intentionally left blank



RISK MANAGEMENT POLICY

Item	Details
Reference:	Corporate Management – 1 - RMP
Status:	Draft
Originator:	Andy Barton
Owner:	Paul Stone
Version No:	7.0
Date:	[To be inserted once approved and published]

Key policy details

Approvals

Item	Date of Approval	Version No.
Consulted with	N/a	
Reviewed by Audit and Governance Committee	7 August 2024	7.0
Approved by Cabinet	24 September 2024	7.0

Policy Location

This policy can be found on NWLDC's website and on the Sharepoint page under current policies tab.

Revision history

Version Control	Revision Date	Summary of Changes
7.0	13 June 2024	<ul style="list-style-type: none"> Corporate Risk Scrutiny Group now renamed Corporate Risk Management Group Minor formatting changes Clarity on which committee reviews the Corporate Risk Register i.e. Audit and Governance Committee as per the Council's Constitution. Graphic added to section 4. Additional text for clarity regarding identifying risk in the appendix Revised format of the risk register in the appendix Role of Members added in the appendix

Policy Review Plans

This policy is subject to a scheduled review once every year or earlier if there is a change in legislation or local policy that requires it.

Distribution

Title	Date of Issue	Version No.
Audit & Governance Committee	7 August 2024	7.0
Cabinet	24 September 2024	7.0
Available on NWL website	[To be confirmed]	7.0

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

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 maintain 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 Management Group (RMG) chaired by Director of Resources. It also refers and reports to Corporate Leadership Team on a quarterly basis, thereby reaching all services in the Council and ensuring senior management oversight and involvement. Progress on Corporate Risk Management is reported to Members through performance reports to the Audit and Governance Committee, at least quarterly. The Corporate Portfolio Holder is the Cabinet member with overall responsibility for risk management.

2.2 The RMG consists of delegates from various council services, each bringing valuable insights to the Council's risk management strategy and the continual evaluation of the Corporate Risk Register.

2.3 Risk management is embedded in the culture of the Council through:

- the continued adoption of the Council's risk management policy statement.
- a nominated officer lead, currently the Director of Resources.
- the RMG 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.
- Briefings and workshops held with Audit and Governance Committee Members.

2.4 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 Council's 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 undertakes a risk-based approach for individual assignments and gives a rating of the level of assurance that is 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

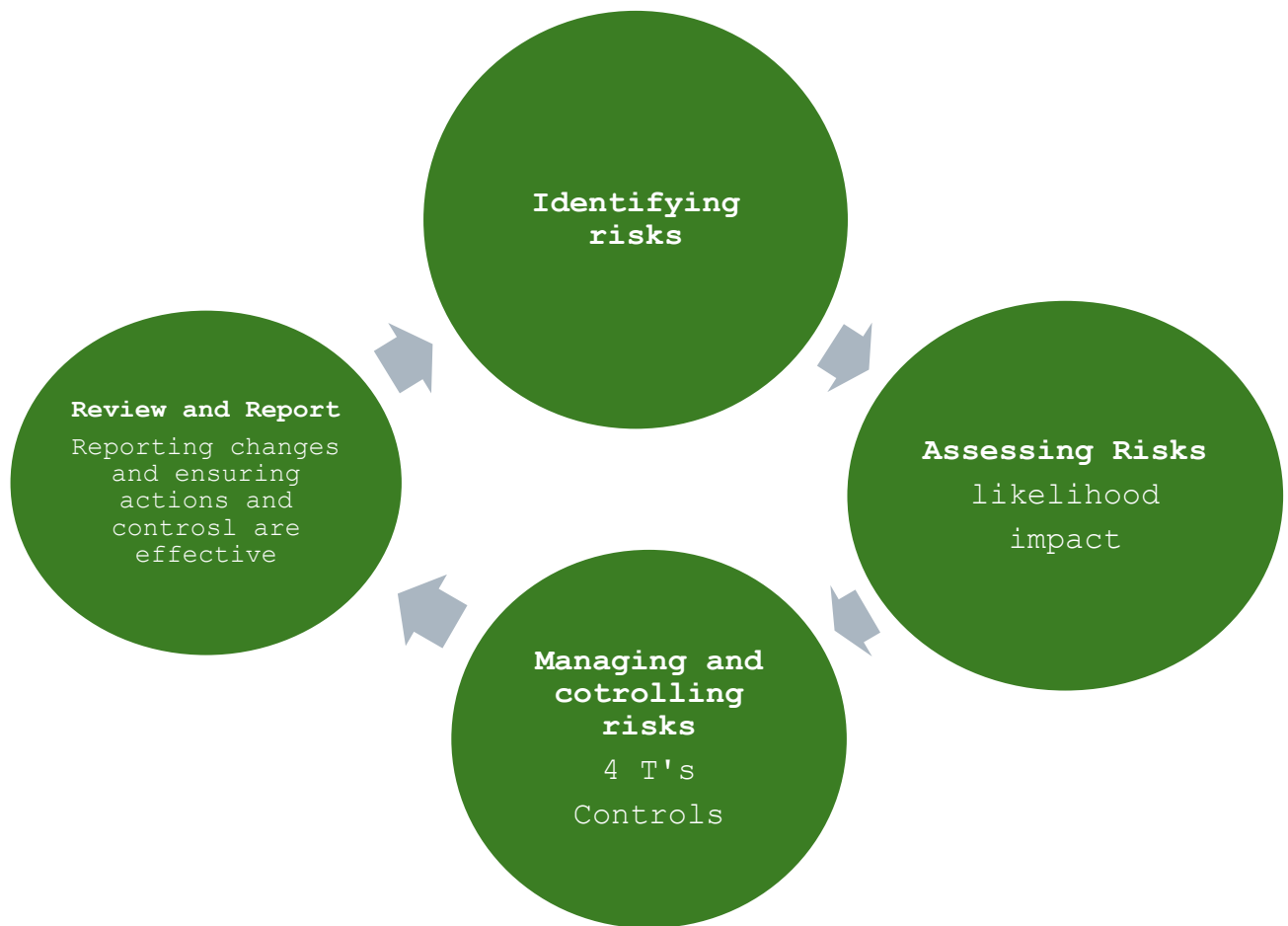
3.1 The Council will strive to maintain its diverse range of services to the community and visitors to the North West Leicestershire area. It will protect and continue to provide these services by ensuring that its assets, both tangible and intangible, are protected against loss and damage. The Council 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 improve 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.
- The CMG will consistently conduct reviews of the Risk Management Policy and the associated processes through the Council's Corporate Leadership Team (CLT) to confirm their ongoing applicability and effectiveness for the Council. This annual review will also assess performance against the aims and objectives set out above. 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.

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 the mitigating 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 RMG 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 toolkits 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.

- Reports to Audit and Governance Committee, in the case of new or changing strategic risks, 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 The Council's risk appetite guides how much risk it is willing to seek or accept to achieve its objectives. The Council recognises it will need to take risks, both in ordinary business and to achieve the priorities set out in the Council Delivery Plan. Good risk management ensures that well informed decisions, are made and the associated risks are understood. By ensuring that risks are properly responded to, the Council will be more likely to achieve its priorities. It also provides control and a high level of due diligence consistent with the Council's responsibilities in managing public money.
- 5.2 The Council recognises effective risk management considers not just threats but also opportunities. So, the 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 the Council seeks a balance between caution and innovation.
- 5.3 The Council's risk appetite reflects its current position; encouraging managed risk taking for minor to moderate level risks but controlling more closely those risks that come

further up the scale. Risk appetite will vary over time depending on the Council's ambitions and priorities and the wider environment in which we work. Resources are aligned to priorities and arrangements are in place to monitor and mitigate risks to acceptable levels.

- 5.4 Beyond Council risk appetite is the Council's risk tolerance. This sets the level of risk that is unacceptable, whatever opportunities might follow. In such instances the Council will aim to reduce the risk to a level that is within its 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 The Council illustrates its risk appetite and tolerance in the grading of risks within the risk register. Risks that are red represents the outer limit of the Council's risk appetite, and those amber or green indicates the tolerance. Where risks are identified as red, ways to reduce these risks will be sought, through the four T's identified above. The Council is unlikely to take risks that will cause a significant negative consequence for the delivery of Council objectives, and only would consider doing so where this is a clear and overarching need to do so.

6. CORPORATE RISK MANAGEMENT GROUP

- 6.1 The Corporate Risk Management 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, for example:

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

- Reduced interruptions to service delivery: fewer surprises!
- Reduced 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
- Reduced 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:

- Ensuring financial sustainability over the medium term.
- Ensuring business continuity and information technology security arrangements futureproof.
- Keeping abreast of Government policy changes, for example the requirements of the Office for Local Government.
- Continually developing the Council's compliance and assurance frameworks to ensure robust decision making.
- Recruitment and retention to key positions across the Council.
- Safeguarding compliance

- Compliance with procurement and contracting regulations
- Responding to emergencies
- Threat of cyber attacks
- Failing to comply with housing landlord regulations
- Failure to meet carbon reduction targets

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 must 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.

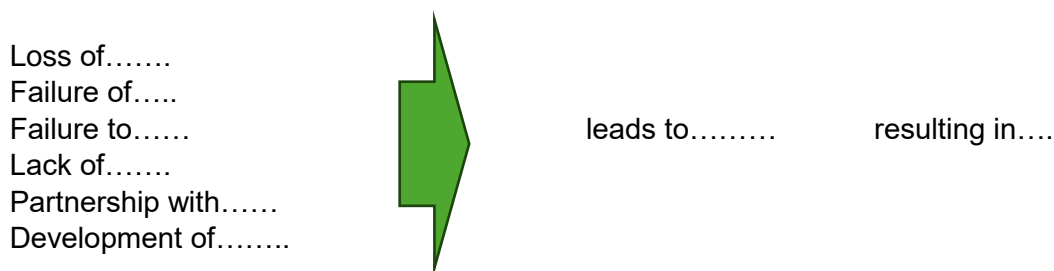
Risk Management cannot be considered in isolation but needs to be an integral part of decision-making and service planning processes of the Council. Risk management must be fully embedded in:

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

(C) identifying and assessing risk

In identifying risks, it is important to consider what could prevent or hinder the Council from achieving its objectives. There are three parts to a risk – an **event** that has a **consequence** that leads to an **impact** on the Council’s objectives.

Typical risk phrasing could be:



You will also need to identify whether the risk is:

- **Strategic:** risks that are significant in size and duration and will impact on the reputation and performance of the Council as a whole and in particular on its ability to deliver its four strategic priorities.
- **Corporate:** risks to corporate systems or processes that underpin the organisation’s overall governance, operation and ability to deliver services.
- **Partnership:** risks to a partnership meeting its objectives or delivering agreed services/projects.
- **Operational:** risks specific to the delivery of individual services/service performance/project.

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	<p>Loss of a service for up to one day. Objectives of individuals are not met. No injuries.</p> <p>Financial loss over £1,000 and up to £10,000. No media attention.</p> <p>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.</p> <p>Service objectives of a service unit are not met.</p> <p>Injury to an employee or member of the public requiring medical treatment.</p> <p>Financial loss over £10,000 and up to £100,000.</p> <p>Adverse regional or local media attention - televised or newspaper report.</p> <p>Potential for a complaint litigation possible. Breaches of regulations / standards.</p>

<p>3. Serious</p>	<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 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>
<p>4. Major</p>	<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. Statutory duties are not achieved.</p> <p>Death of an employee or member of the public. Financial loss over £1m.</p> <p>Adverse national media attention - national televised news report.</p> <p>Litigation almost certain and difficult to defend. 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

Ref	Risk description	Inherent Risk			Risk Response	Risk Owner	Residual Risk		
		Likelihood	Impact	Severity score			Likelihood	Impact	Severity
CR1	Name of Risk Risk Consequence	4	3	12	Treat		3	2	6
Existing Controls	<ul style="list-style-type: none"> 								
Planned mitigating actions				Delivery timescales					
Comments and progress on actions									

(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.

Corporate Leadership Team (CLT) – 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 and Organisational Development – 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 Management 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.

(G) Roles of Members

Audit and Governance Committee The role in addressing outstanding internal audit recommendations is multifaceted and crucial for the integrity of an organisation's governance and risk management frameworks. By actively pursuing the resolution of outstanding recommendations, audit committee members help to strengthen the organization's controls and risk management practices.

The Corporate Risk Register is reviewed by CLT on a quarterly basis. Where the discussion reveals that one or more of the criteria outlined below is met, then the relevant Director or Head of Service may be invited to an upcoming Audit and Governance Committee to discuss in more detail if needed.

Criteria for inviting the Director or Head of Service to the Audit and Governance Committee:

- There has been limited progress on the implementation of mitigating actions, over at least two successive quarters
- There is a deteriorating direction of travel, with either increased likelihood / impact of the risk.
- There are significant or emerging likely impacts from a budget perspective, reputational view, or a failure to meet statutory requirements in the area of risk.
- The risk has been considered by the Corporate Risk Management Group and is recommended for review by Audit and Governance Committee.

- There is a forecasted change in the context of the risk (i.e. national policy changes), which requires a review of the likelihood and impact, alongside a challenge on the effectiveness of any current controls

Equality Analysis

Completion of Equality Impact Assessment (EIA) Form

Has an EIA form been completed as part of creating / reviewing / amending this policy?	Please tick: Yes <input checked="" type="checkbox"/> No <input type="checkbox"/>
If yes, where can a copy of the EIA form be found?	<u>Available on request from the Equalities Officer</u>
If no, please confirm why an EIA was not required?	N/a



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

Item	Details
Reference:	Internal Audit – 4 – RIPA
Status:	Final
Originator:	Internal Audit Manager
Owner:	Internal Audit Manager
Version No:	1.5
Date:	[To be inserted once approved and published]

Key policy details

Approvals

Item	Date of Approval	Version No.
Consulted with – no consultation took place as part of the review in 2024		
Reviewed by Audit and Governance Committee	7 August 2024	1.5
Approved by Cabinet	24 September 2024	1.5

The policy owner has the authority to make the following minor changes without approval:

None

Policy Location

This policy can be found at NWLDC website and the Sharepoint page under current policies tab.

Revision history

Version Control	Revision Date	Summary of Changes
1.1	May 2020	
1.2	June 2021	
1.3	June 2022	No changes
1.4	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.
1.5	July 2024	Change to date Home Office Codes of Practice last published.

Policy Review Plans

This policy is subject to a scheduled review once every year or earlier if there is a change in legislation or local policy that requires it.

Distribution

Title	Date of Issue	Version No.
Audit & Governance Committee	7 August 2024	1.5
Cabinet	24 September 2024	1.5
Available on NWL website	[To be confirmed]	1.5

	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 February 2024) 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 December 2022). 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 February 2024) 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 three-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, 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

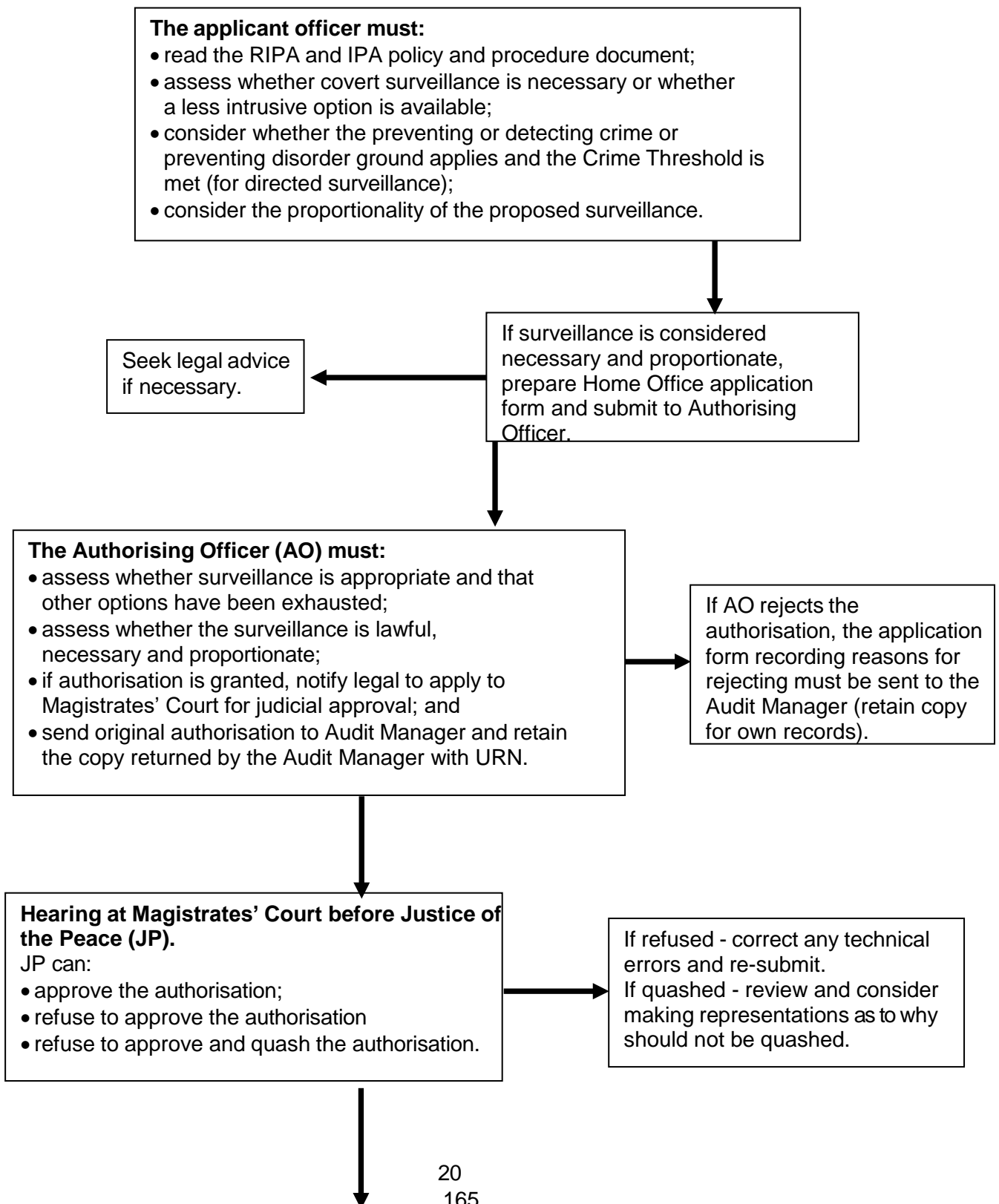
- 14.10 Departments must ensure that arrangements are in place for the handling, storage and destruction of material obtained through the use of **covert** surveillance, a CHIS and/or the acquisition of communications data which accord with the Council's Information Management Policy. Records will be 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.

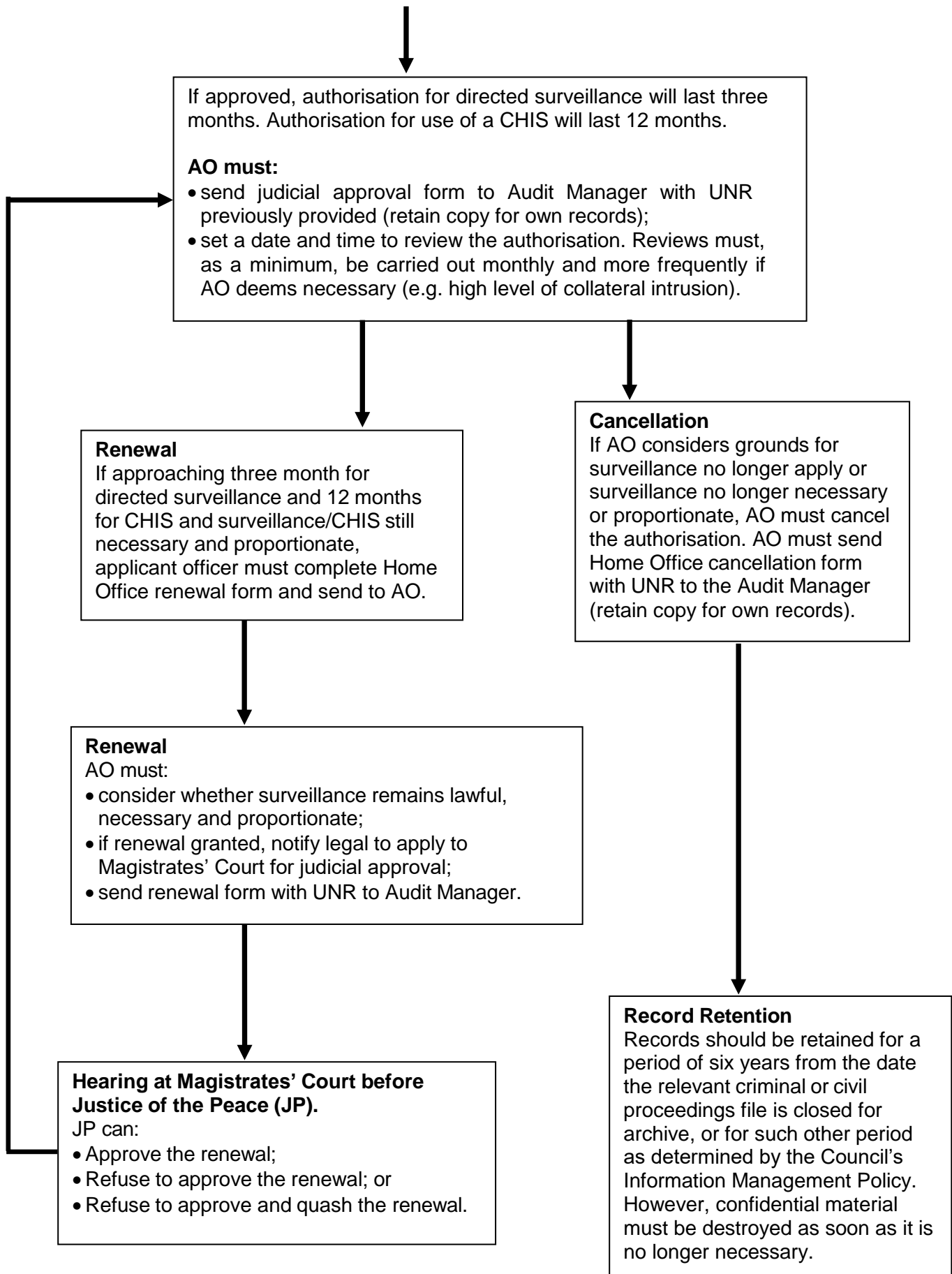
15. REVISION HISTORY

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

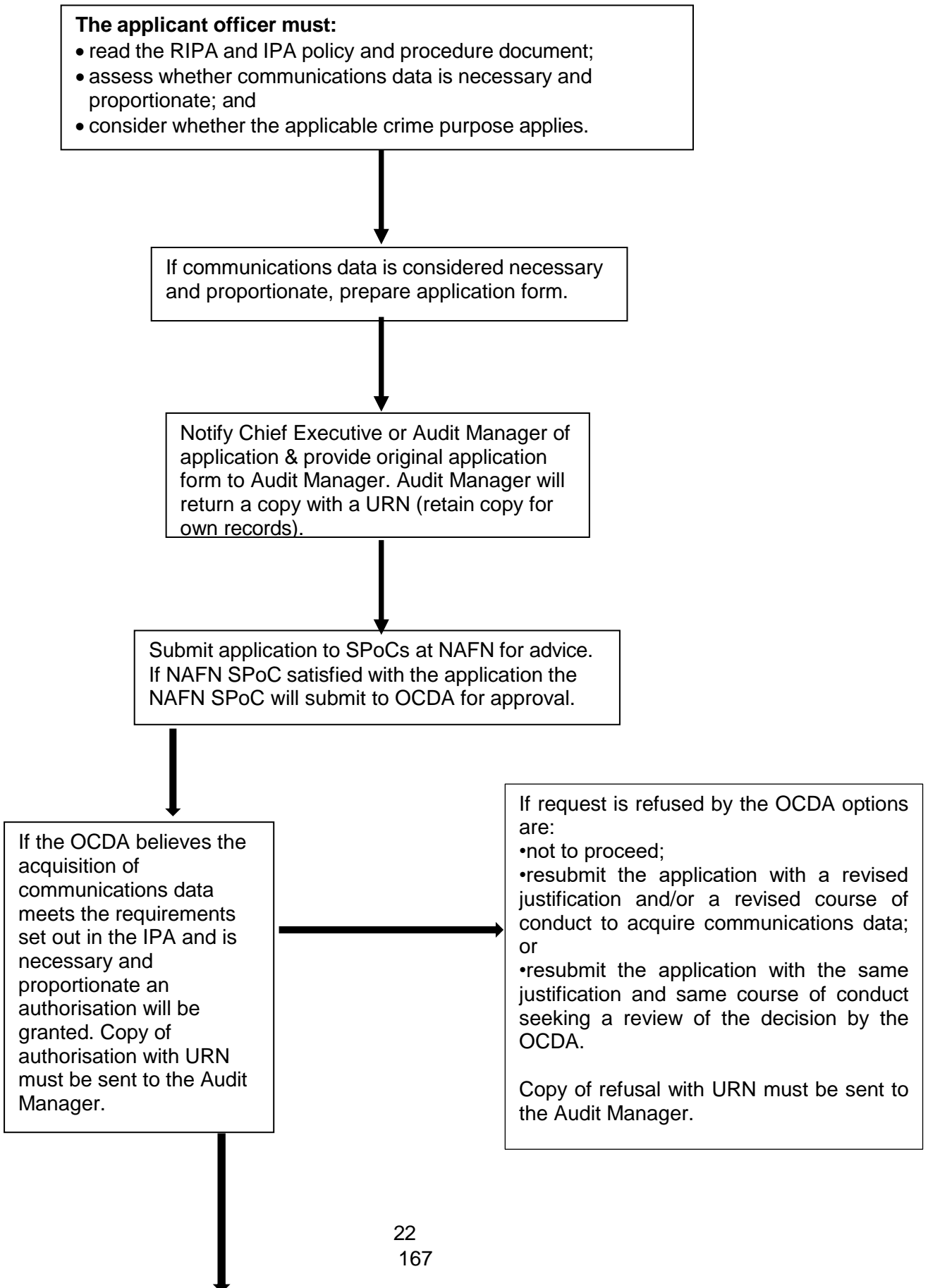
RIPA - AUTHORISATION OF DIRECTED SURVEILLANCE / USE OF A CHIS PROCEDURE

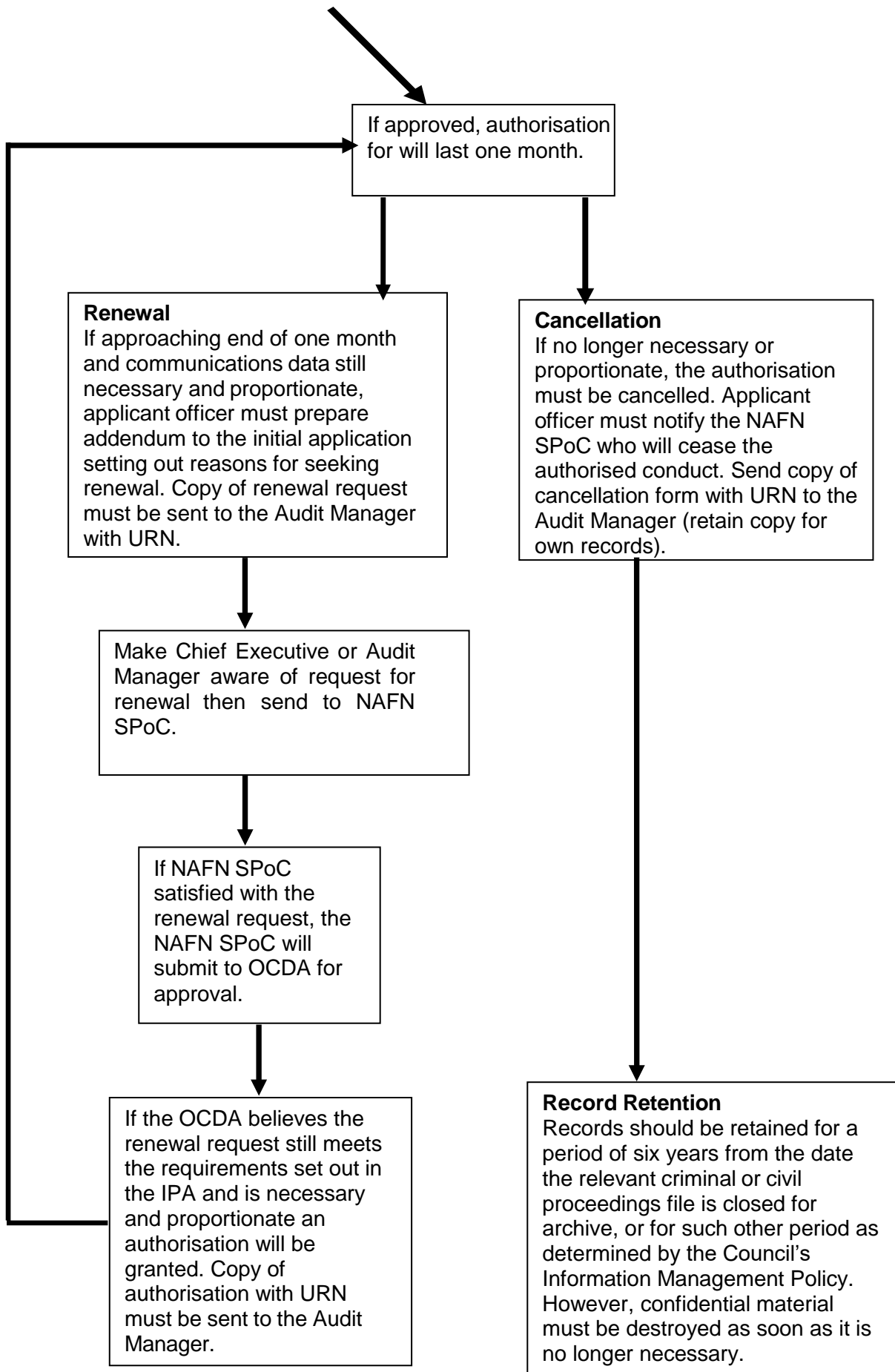
(Note: Note: Only the Chief Executive may authorise the use of a juvenile or vulnerable individual as a CHIS)





IPA - COMMUNICATIONS DATA AUTHORISATION PROCESS





Equality Analysis

Completion of Equality Impact Assessment (EIA) Form

Has an EIA form been completed as part of creating / reviewing / amending this policy?	Please tick: Yes <input checked="" type="checkbox"/> No <input type="checkbox"/>
If yes, where can a copy of the EIA form be found?	With the Equality, Diversity and Inclusion Officer
If no, please confirm why an EIA was not required?	N/A

This page is intentionally left blank



Local Code of Corporate Governance

Item	Details
Reference:	LCCG-01
Status:	Final
Originator:	Head of Finance
Owner:	Head of Finance
Version No:	7
Date:	[To be inserted once approved and published]

Key policy details

Approvals

Item	Date of Approval	Version No.
Consulted with	N/a	
Reviewed by Audit and Governance Committee]	07/08/2024	7
Approved by Cabinet	24/09/2024	7

The policy owner has the authority to make the following minor changes without approval

- Minor amendments as a result of changes in national policy and changes to local priorities

Policy Location

This policy can be found on the Council's website.

Revision history

Version Control	Revision Date	Summary of Changes
1	2009	
2	October 2017	
3	May 2020	
4	June 2021	
5	May 2022	
6	July 2023	New section on the current challenges facing the Council Changes to formatting
7	July 2024	Changes to formatting

Policy Review Plans

This policy is subject to a scheduled review once a year or earlier if there is a change in legislation or local policy that requires it.

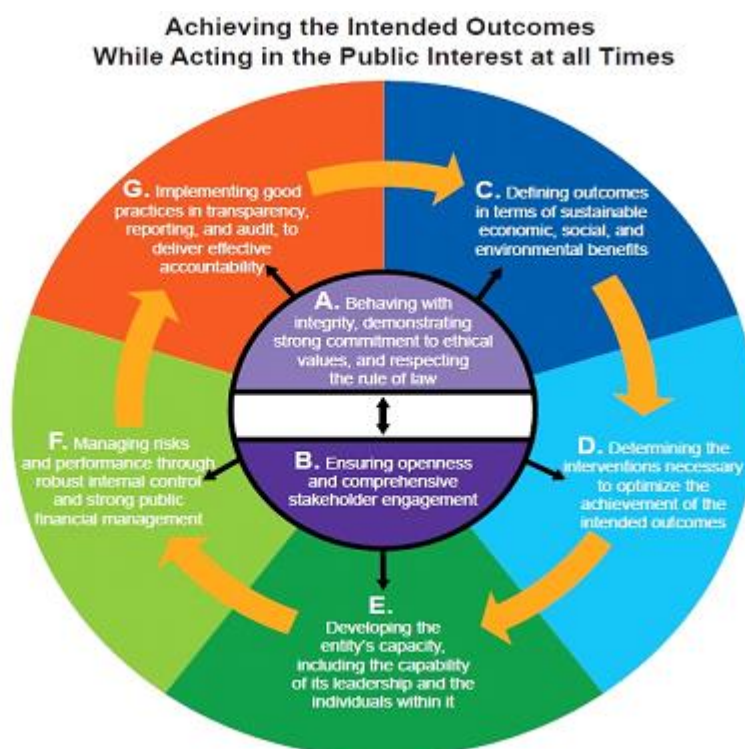
Distribution

Title	Date of Issue	Version No.
-------	---------------	-------------

Audit and Governance Committee	7 August 2024	7
Cabinet	24 September 2024	7
Website updated	[To be confirmed]	7

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 CIPFA in association with the Society of Local Authority Chief Executives (SOLACE) has published their Framework entitled 'Delivering Good Governance in Local Government 2016'.
- 1.3 The diagram below illustrates¹ 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.



¹ Delivering Good Governance in Local Government 2016

- 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:

[The Seven Principles of Public Life - GOV.UK \(www.gov.uk\)](http://www.gov.uk)

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 the Council 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 of Good Governance in Public Services.

Principle A – Behaving with integrity, demonstrating strong commitment to ethical values, and respecting the rule of rule	
Sub-Principle	The Council is committed to:
Behaving with Integrity	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	
Sub-Principle	The Council is committed to:
Ensuring an open culture through demonstrating, documenting and communicating the organisation’s commitment to openness	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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

Sub-Principle	The Council is committed to:
Defining outcomes	<ul style="list-style-type: none"> • 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 user expectations effectively with regard to determining priorities and making the best use of the resources available.
Sustainable economic, social and environmental benefits	<ul style="list-style-type: none"> • 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	
Sub-Principle	The Council is committed to:
Determining interventions	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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

Sub-Principle 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 Council’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 Council 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.

	<ul style="list-style-type: none"> • 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	
Sub-Principle	The Council is committed to:
Managing Risk	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Aligning the risk management strategy and policies on internal control with achieving the objectives. • Evaluating and monitoring the Council’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	<ul style="list-style-type: none"> • 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 Finance Management	<ul style="list-style-type: none"> • 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

Sub-Principle	The Council is committed to:
Implementing good practice in transparency	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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.

Equality Analysis

Completion of Equality Impact Assessment (EIA) Form

Has an EIA form been completed as part of creating / reviewing / amending this policy?	Please tick: Yes <input type="checkbox"/> No <input type="checkbox"/>
If yes, where can a copy of the EIA form be found?	
If no, please confirm why an EIA was not required?	

This page is intentionally left blank



Data Protection Policy

Item	Details
Reference:	Information Governance-1 DPP
Status:	Draft
Originator:	Head of Legal & Support Services
Owner:	Data Protection Officer
Version No:	1:1
Date:	[To be inserted once approved and published]

Key policy details

Approvals

Item	Date of Approval	Version No.
Consulted with N/A		
Reviewed by Audit and Governance Committee	7 August 2024	1:1
Approved by Cabinet	24 September 2024	1:1

The policy owner has the authority to make the following minor changes without approval.

Operational Changes - any modification in data protection procedures or required alignments with other documents within the Information Governance Framework.

Regulatory Decisions - when Court or regulatory decisions impact information security practices.

Guidance Changes - If there are changes in regulatory guidance related to data protection the policy owner should review and update this policy accordingly.

Policy Location

This policy can be found at NWLDC's website and the Sharepoint page under current policies tab.

Revision History

Version Control	Revision Date	Summary of Changes
1:1	July 2024	Creation of Document

Policy Review Plans

This policy is subject to a scheduled review once every year or earlier if there is a change in legislation or local policy that requires it.

Distribution

Title	Date of Issue	Version No.
Distributed to Cabinet	24 September 2024	1:1
Published on NWLDC Website	TBC	1:1

Data Protection Policy

1. Introduction

North West Leicestershire District Council ('the Council') has responsibilities under the Data Protection Act 2018(DPA 2018), UK General Data Protection Regulation (UK GDPR), Local Government Acts and the Human Rights Act 1998 to protect rights of privacy and ensure that personal data is sufficiently protected when it is being processed.

The Council is required as part of its overall information governance structure to ensure that appropriate controls are implemented and maintained in the collection and use of personal information pertaining to its customers, clients and staff and that these are in accordance with the requirements of the current data protection law (the DPA 2018 and the UK GDPR along with other legislation).

In most cases the Council will be the data controller for the personal data it processes. A data controller is the organisation or person who determines and controls the purpose for the processing of personal data. In some cases, the Council may be a joint data controller with another organisation.

There may also be circumstances in which the Council has appointed a third party to process data on its behalf and in such circumstances that party will be a data processor but the Council will remain the data controller.

This policy sets out the Council's approach to complying with the above legislation in relation to data protection and forms part of the Council's Information Governance Framework, which applies to all staff including employees, councillors, agency staff, contractors, volunteers or any other persons who have access to, or use the Council's information concerning personal data.

2. Scope

This policy forms part of the Council's Information Governance Framework, which applies to all staff including employees, councillors, agency staff, contractors, volunteers or any other persons who have access to, or use the Council's information.

The scope of this policy requires compliance with the principles defined in law.

Personal data is defined as:

Any information related to an identified or identifiable living natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (Article 4 UK GDPR).

Special category personal data is defined as personal data relating to any of the following (Article 9 UK GDPR):

- Racial or ethnic origin.
- Political opinions.
- Religious or Philosophical beliefs.
- Trade Union membership.

- Genetic or biometric data for the purpose of uniquely identifying a natural person.
- Data concerning health.
- Sex life or sexual orientation.

Criminal Offence data is personal data relating to criminal convictions and offences or related security measures (Article 10 UK GDPR).

Criminal offence data can only be processed:

- Under the control of official authority, or
- If authorised by domestic law - this means that one of the conditions in schedule 1 of the DPA is met.

All personal data must be protected. Special category personal data and criminal offence data may require special protection measures.

3. Principles of Good Practice

The UK GDPR includes principles which must be adhered to whenever personal data is processed. Processing includes obtaining, recording, using, holding, disclosing and deleting personal data.

All personnel processing personal data must ensure they adhere to the principles as defined in the data protection law which require that personal data is:

- Used fairly lawfully and transparently.
- Used for specific explicit purposes.
- Used in a way that is adequate, relevant and limited to only what is necessary.
- Accurate and where necessary kept up to date.
- Kept for no longer than is necessary.
- Handled in a way that ensures appropriate security including protection against unlawful or unauthorised processing, access, loss destruction or damage.

4. Access and use of Personal Data

This policy applies to everyone that has access to personal data and includes any third party or individual who conducts work on behalf of North West Leicestershire District Council or who has access to personal data for which the council is responsible and who will be required contractually or otherwise to comply with this policy.

The Policy is also applicable to Members who create records in their capacity as representatives of the council.

It is an offence for any person to knowingly or recklessly obtain, procure or disclose personal data, without the permission of the data controller.

All data subjects are entitled to:

- Be informed about how data is being used.
- Access personal data.
- Have correct data updated.
- Have data erased.
- Stop or restrict the processing of data.
- Data portability (allow data subjects to get and reuse data for different services).

- Object to how data is being processed in certain circumstances.

The above rights are not absolute and only apply in certain circumstances

The Council will process all personal data in accordance with the relevant legislation. Where the Council is seeking to pursue a new project or process that involves the use of personal data, a data protection impact assessment will be carried out to assist the Council in systematically analysing, identifying and minimising the data protection risks.

The Council will only process personal data where it complies with the data protection principles under the legislation and in doing so will only process the minimum personal data required for the intended purpose. The Council will also seek to use anonymised data where appropriate to do so in order to avoid the retention of personal data where it is not necessary to retain it.

In the collection and retention of personal data, the Council will take reasonable steps to ensure that the personal data held is accurate, up-to-date and not misleading. All personal data will be retained in accordance with the Council's retention schedule.

The Council holds an information asset register, which includes information about data processing activities and any systems that process personal information.

Personal data will be processed and stored by the Council in accordance with the Council's IT Security Policy. Where the Council appoints a third party to process personal data on its behalf, it will enter into a data processing agreement with the third party to ensure that the personal data is sufficiently protected. The Council will ensure that information processed by third parties is done so in line with legal requirements and good practice.

The Council has privacy notices which explain why it collects personal data, how that personal data is used and shared (if applicable), and the rights that people have over their personal data.

5. Sharing Personal Data

There may be a need for the Council to share personal data that it holds with another party, in which case it will only do so where it has a legal obligation, power or permission to do so. Where appropriate, individuals will be informed that their personal data is being shared and any personal data shared will be undertaken confidentially and securely.

The Council will ensure that data sharing agreements are in place (where appropriate) to set out the terms on which personal data will be shared with another party. The Council also maintains a register of data sharing arrangements.

Where personal data is being transferred, the Council will endeavour not to transfer personal data outside of the European Union, to third countries or international organisations unless there is a legal requirement to do so or it can be evidenced that appropriate safeguards are in place as required by data protection legislation. In the event that international transfers are being considered, a data protection impact assessment will be undertaken.

Personal data within the Council will only be accessed by those employees that need to access the information for their role and business need. There may be circumstances in which it is appropriate to limit access to certain personal data to specific members of staff, due to the sensitive nature of the personal data and/or how it is being used.

6. Information Security Incidents

The Council has a procedure for reporting, logging and investigating information security incidents. Where such information security incidents indicate that there has been a breach of data protection legislation, the Council will consider whether it is appropriate and necessary to report the breach to the Information Commissioner's Office in accordance with the Council's procedure.

All incidents of a personal data breach must be reported to the Data Protection Officer via the [staff portal](#). As much information as possible should be provided and reported as soon as or within '24hrs' of the incident being identified.

An information security incident includes but is not restricted to the following:

- The loss or theft of data or information.
- The transfer of data or information to those who are not entitled to receive that information.
- Attempts (either failed or successful) to gain unauthorised access to data or information storage or a computer system.
- Changes to information or data or system hardware, firmware or software characteristics without the Council's knowledge.
- The unauthorised use of a system for the processing or storage of any data by any person.

7. CCTV and Surveillance Camera Technologies

The Council recognises that images and audio recordings of identifiable individuals captured by surveillance camera systems (e.g. CCTV; body worn cameras, drones etc) are personal data and will be subject to the same provisions and safeguards afforded by data protection legislation as other types of personal information.

The Council has a CCTV policy which sets out how it will ensure that the data protection legislation will be complied with and takes account of the Surveillance Camera Commissioner's Code of Practice.

CCTV and surveillance camera technologies will only be used where it is necessary and proportionate to achieve its objective. The introduction of new CCTV and surveillance camera technologies will be subject to a data protection impact assessment.

Further Information

The Information Commissioner's Office (ICO) is the independent authority set up to monitor compliance with the Data Protection Act and General Data Protection Regulation. It also issues guidance and good practice notes. You can contact the ICO here [Information Commissioner's Office \(ICO\)](#).

The ICO can consider complaints about an organisations failure to comply with the Act and regulations following the initial reply from that organisation.

Equality Analysis

Completion of Equality Impact Assessment (EIA) Form

Has an EIA form been completed as part of creating / reviewing / amending this policy?	Please tick: Yes <input checked="" type="checkbox"/> No <input type="checkbox"/>
If yes, where can a copy of the EIA form be found?	Available upon request
If no, please confirm why an EIA was not required?	

This page is intentionally left blank



Information Governance Framework

Item	Details
Reference:	Information Governance -1-IGF
Status:	Draft
Originator:	Head of Legal & Support Services
Owner:	Data Protection Officer
Version No:	1:1
Date:	[To be inserted once approved and published]

Key policy details

Approvals

Item	Date of Approval	Version No.
Consulted with N/A		
Reviewed by Audit and Governance Committee	7 August 2024	1:1
Approved by Cabinet	24 September 2024	1:1

The policy owner has the authority to make the following minor changes without approval.

Operational Changes - any modification in data protection procedures or required alignments with other documents within the Information Governance Framework.

Regulatory Decisions - when Court or regulatory decisions impact information security practices.

Guidance Changes - If there are changes in regulatory guidance related to data protection the policy owner should review and update this policy accordingly.

Policy Location

This policy can be found at the Council's website and SharePoint page under current policies tab.

Revision History

Version Control	Revision Date	Summary of Changes
1:1	July 2024	Creation of Document

Policy Review Plans

This policy is subject to a scheduled review once every year or earlier if there is a change in legislation or local policy that requires it.

Distribution

Title	Date of Issue	Version No.
Distributed to Cabinet	24 September 2024	1:1
Published on NWLDC website	TBC	

Information Governance Framework

1. Introduction

North West Leicestershire District Council (the “Council”) processes information in a variety of ways in order to effectively and efficiently deliver services to its customers. The Council recognises that good information management is key to ensuring that information is used appropriately and that the relevant legislation and guidance is complied with. It is of paramount importance that information is efficiently managed and that appropriate accountability, standards, policies and procedures provide a robust governance framework for effective information management.

This Information Governance Framework captures the Council's approach to holding, obtaining, recording, using and sharing information, as well as how the Council ensures that sufficient technical and organisational measures are in place to safeguard it. It includes the principles of information governance, policies and procedures, roles and responsibilities and training requirements.

2. Scope

This Information Governance Framework and the documents within it apply to all staff including employees, councillors, agency staff, contractors, volunteers or any other persons who have access to, or use the Council's information. It applies to all types of information and data, both electronic and manual, which is held, processed or transmitted by the Council.

Information includes all paper and electronic records, whether that be raw or analysed data, informal or formal documents, customer or other records and any other type of content.

Non-compliance with this Framework and associated policies could potentially expose the Council and/or its customers to unacceptable risk.

3. Principles

Information governance spans a variety of activities that the Council undertakes. The following principles apply to all information held by the Council and form the foundation of good information governance:

1. Information Rights - we have legal obligations to provide information when requested.
2. Records Management - we must retain information for an appropriate period of time and manage records effectively.
3. Data Protection - we are required to have appropriate safeguards in place to protect our information, especially personal data.
4. Information Security - we must ensure that we have technical measures in place to ensure that the handling of our information is secure.



It is important that staff understand what information they need to do their job and how these principles apply to the information they handle.

4. Policies and Procedures

In line with the above principles, this Information Governance Framework includes four key policies:

1. Information Rights Policy
2. Records Management Policy
3. Data Protection Policy
4. Information Security Policy

Underpinning these policies are internal standards, procedures and guidance that set out how the policy requirements will be achieved.

Information Governance Framework

Policies

These set out why requirements are in place

Our key policies are:

Information Rights Policy

1. Records Management Policy

2. Data Protection Policy

3. Information Security Policy

Standards

These set out what the requirements are

These include:

Retention Schedule

Information Asset Register

Data Sharing Register

Acceptable Use

Procedures and Guidance

These set out how requirements are met

These include:

Data Breach and Information Security Incident Procedure

Information Requests Guidance

Procedure for Information Sharing

Subject Access Requests Guidance

CCTV and Surveillance Camera Technologies Procedure

Employee Monitoring Procedure

5. Roles and Responsibilities

The **Senior Information Risk Owner (“SIRO”)** is the Head of Legal and Support Services.

The SIRO has the following responsibilities:

- To be accountable for risk management in relation to information governance at the Council;
- To take overall ownership of the organisation's information risk approach, including the information governance framework; and
- To oversee the Data Breach and Information Security Incident Procedure and the Council's compliance in relation to dealing with information security incidents (data breaches).

The SIRO is supported by the Council's **Data Protection Officer (“DPO”)**, who has the following key responsibilities:

- To monitor compliance across the organisation to ensure that the Council meets its obligations under data protection legislation and applicable guidance;
- To ensure that the Council develops, implements, reviews and updates measures to comply with data protection legislation;
- To ensure that the Council has an appropriate training programme to make members of staff aware of their responsibilities in relation to information governance and data protection;
- To deal with any complaints in relation to the processing of personal data;
- To be responsible for the Council's approach to dealing with information security incidents and ensure that any personal data breaches are fully investigated and reported through the appropriate channels if appropriate; and
- To act as the contact point for the ICO on issues relating to the processing of personal data and to co-operate with the ICO in relation to any enquires and/or investigations.

The DPO is part of the **Information Governance Team** that manages information governance on a day-to-day basis across the organisation and supports staff in how they handle information.

Information Asset Owners

Information Asset Owners are team managers with responsibilities for service areas. Team managers in their capacity as Information Asset Owners are responsible for ensuring that staff and contractors know of their responsibilities, understand and follow procedures for handling, releasing and disposing of information. They will consult with the DPO as required.

Surveillance Camera System Senior Responsible Officer

The Community Safety Team Leader is responsible for surveillance cameras and their systems across the Council.

IT Security

The ITC team manager is responsible for Information security for the Council.

6. Training and Guidance

All staff must complete annual training on data protection. This training is delivered electronically via an e-module for the majority of staff. Where members of staff do not have IT access, alternative arrangements are in place.

Training specific to managers will be delivered to Team Managers and CLT as part of the Council's annual Corporate Governance Programme, as and when required.

Training for specific service areas will also be delivered on an ad hoc basis, as and when circumstances demand.

The Council has an internal information governance toolkit for staff to use to access the documents within the framework, including relevant procedures and guidance.

In addition to the above, the Information Governance Team promote good information governance via a variety of methods, including internal blogs, bulletins and where necessary, corporate emails.

7. Monitoring and Review

This Information Governance Framework will be reviewed each year to coincide with the review of the Council's Corporate Governance policies. It will also be updated and/or amended as necessary to reflect changes in legislation and best practice.

8. Relevant Legislation

The following legislation is relevant to this Information Governance Framework:

- The UK General Data Protection Regulation
- Data Protection Act 2018
- Human Rights Act 1998
- Protection of Freedoms Act 2012
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Local Government Acts
- Computer Misuse Act 1990

Equality Analysis

Completion of Equality Impact Assessment (EIA) Form

Has an EIA form been completed as part of creating / reviewing / amending this policy?	Please tick: Yes <input checked="" type="checkbox"/> No <input type="checkbox"/>
If yes, where can a copy of the EIA form be found?	Available upon request
If no, please confirm why an EIA was not required?	



Information Security Policy

Item	Details
Reference:	Information Governance-1-ISP
Status:	Draft
Originator:	Head of Legal & Support Services
Owner:	Data Protection Officer
Version No:	1:1
Date:	[To be inserted once finalised]

Key policy details

Approvals

Item	Date of Approval	Version No.
Consulted with N/A		
Reviewed by Audit and Governance Committee	7 August 2024	1:1
Approved by Cabinet	24 September 2024	1:1

The policy owner has the authority to make the following minor changes without approval.

Operational Changes - any modification in information security or technology procedures or required alignments with other documents within the Information Governance Framework.

Regulatory Decisions - when Court or regulatory decisions impact information security practices.

Guidance Changes - If there are changes in regulatory guidance related to information security the policy owner should review and update this policy accordingly.

Policy Location

This policy can be found on NWLDC's website and Sharepoint page under current policies tab.

Revision History

Version Control	Revision Date	Summary of Changes
1:1	24 September 2024	Creation of Document

Policy Review Plans

This policy is subject to a scheduled review once every year or earlier if there is a change in legislation or local policy that requires it.

Distribution

Title	Date of Issue	Version No.
Distributed to Cabinet	24 September 12024	1:1
Published on NWLDC Website	TBC	1:1

Information Security Policy

1. Introduction

This Information Security Policy outlines our commitment to protect North West Leicestershire District Council's ("The Council") information assets against all internal, external, accidental or deliberate threats and minimise risks related to information security.

Information security is characterised as the preservation of:

- Confidentiality - ensuring that information is only available to those who have authorisation to have access.
- Integrity - safeguarding the accuracy and completeness of information and processing methods.
- Availability - ensuring that authorised users have access to information and associated assets when required.

The confidentiality, integrity and availability of data is vital to Council operations and public trust.

Information security management is an ongoing cycle of activity aimed at continuous improvement in response to changing threats and vulnerabilities. It can be defined as the process of protecting information from unauthorised access, disclosure, modification or destruction and is vital for the protection of information and the Council's reputation.

The Council has a statutory obligation to have sound information security arrangements in place. The Data Protection Act 2018 emphasises the importance of technical and organisational measures to ensure secure processing of personal data. The security principle under the UK GDPR emphasises processing personal data securely through appropriate technical and organisational measures.

2. Purpose

The purpose of this policy is to:

- Establish guidelines and procedures for safeguarding information within the council.
- Ensure the protection of all information in all its forms.
- Establish a framework for managing information security.
- Promote a secure information culture within the Council.

3. Scope

This policy forms part of the Council's Information Governance Framework, which applies to all staff including employees, councillors, agency staff, contractors, volunteers or any other persons who have access to, or use the Council's information systems and data. It applies to all information assets as defined in the Council's Records Information Management Policy.

Application of this policy applies throughout the information lifecycle from acquisition/creation, through to utilisation storage and disposal.

4. Responsibilities

The Senior Information Risk Owner (SIRO)

- is responsible for managing Information Security within the authority.

The IT Manager

- is responsible for the implementation of this policy.

All employees

- must adhere to this policy and report any security incidents promptly
- are responsible for protecting information assets and following security best practices.

5. Authorised Use

Access to information for which the Council is responsible is permitted in support of the Council's areas of business or in connection with a service utilised by the Council. Authorised users are defined as Council employees, elected members, authorised contractors, temporary staff and partner organisations.

6. Information Classification

Asset classification and control is an essential requirement, which will ensure the Confidentiality, Integrity and Availability of information used by the council. An information classification system is used to define appropriate protection levels and to communicate the need for special handling measures. Each information asset should be classified to indicate its sensitivity and to identify the controls required to protect it. All information assets must be classified based on its sensitivity and criticality for the council's business. Employees should follow the Information Classification Procedure to determine the appropriate information handling procedures for each classification level. The classification levels are:

- **Sensitive** - sensitive information where consideration should be given to who it is shared with.
- **Official Sensitive** (personal) – sensitive information concerning individuals.
- **Official Sensitive** (commercial) - sensitive information with commercial implications.
- **Legal Privilege** - confidential communications between lawyers and clients when the purpose is to seek legal advice.
- **Official** – any information not marked (not covered under other categories and no special handling required).

7. Data Retention

The Council recognises the importance of managing data retention effectively to ensure compliance with legal requirements, operational needs and privacy considerations. We have a data Retention Schedule with principles that guide our retention practices. Employees should adhere to the requirements of this schedule. Please Contact the Data Protection Officer for any queries relating to data retention.

8. Access Control

- Access to information will be based on the principle of least privilege and need to know basis.
- User access rights should be reviewed periodically and revoked promptly when no

longer necessary.

9. Password Management

- Employees must use strong unique passwords for their accounts.
- Regular password changes are encouraged.
- Multi- Factor authentication (MFA) should be implemented wherever possible.

10. Data Encryption

- Sensitive data in transit (e.g emails, network traffic) and at rest (e.g stored files) must be encrypted.
- Encryption protocols and algorithms should align with industry best practices.

11. Incident Response

- 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.
- The personal data breach process and reporting requirements still apply to security incidents that amount to or include personal data breaches. Any Security incident that may have potential to lead to disciplinary action will involve the appropriate involvement and consultation with head of Human Resources and Organisation Development and or (depending on the nature of the incident) the Audit services manager.

12. Physical Security

- Access to physical premises should be restricted.
- Visitors must sign in and be escorted whilst on site.

13. Training and Awareness

- Regular security awareness sessions will be conducted for all staff.
- Employees will be informed about phishing risks, social engineering and safe computing practices.

14. Third-Party Vendors

- Third-party vendors handling our data must adhere to our security standards.
- Contracts with vendors should contain information security clauses.

15. Compliance with Legal and Contractual Obligations

The Council will abide by all UK legislation relating to information storage and processing including:

- Data Protection Act 2018
- UK General Data Protection Regulation 2018
- The Freedom of Information Act 2000
- The Environmental Information Regulations 2004
- The Computer Misuse Act 1990
- The Human Rights Act 1998

- The Copyright Designs and Patents Act 1988

Compliance

Non-compliance with this policy may result in disciplinary action.

Regular audits will assess adherence to this policy.

Equality Analysis

Completion of Equality Impact Assessment (EIA) Form

Has an EIA form been completed as part of creating / reviewing / amending this policy?	Please tick: Yes <input checked="" type="checkbox"/> No <input type="checkbox"/>
If yes, where can a copy of the EIA form be found?	Available upon request.
If no, please confirm why an EIA was not required?	

This page is intentionally left blank



Information Rights Policy

Item	Details
Reference:	Information Governance -1-IRP
Status:	Draft
Originator:	Head of Legal & Support Services
Owner:	Data Protection Officer
Version No:	1:1
Date:	[To be inserted once finalised]

Key policy details

Approvals

Item	Date of Approval	Version No.
Consulted with N/A		
Reviewed by Audit and Governance Committee	7 August 2024	1:1
Approved by Cabinet	24 September 2024	1:1

The policy owner has the authority to make the following minor changes without approval.

Operational Changes - any modification in information rights procedures or required alignments with other documents within the Information Governance Framework.

Regulatory Decisions - when Court or regulatory decisions impact information rights practices.

Guidance Changes - If there are changes in regulatory guidance related to information rights the policy owner should review and update this policy accordingly.

Policy Location

This policy can be found on the Council's website and the Sharepoint page under current policies tab.

Revision History

Version Control	Revision Date	Summary of Changes
1:1	July 2024	Creation of Document

Policy Review Plans

This policy is subject to a scheduled review once every year or earlier if there is a change in legislation or local policy that requires it.

Distribution

Title	Date of Issue	Version No.
Distributed to Cabinet	24 September 2024	1:1
Published on website	TBC	

Information Rights Policy

1. Introduction

Under the Data Protection Act 2018 individuals have various rights in relation to the information that North West Leicestershire District Council (the “Council”) processes about them.

Members of the public can also request information from the Council under the Freedom of Information Act 2000(FOI) The Environmental Information Regulations 2004 apply to all information which relates to the environment, in its broadest sense, including land, air, water, soil, buildings, animals and people, pollution of all kinds, waste, health and safety. This also includes reports, measures and analysis of environmental information. Whereas the Freedom of Information Act 2000 applies to all other information.

This policy sets out the Council’s approach to complying with this legislation in relation to information rights.

2. Scope

This policy forms part of the Council’s Information Governance Framework, which applies to all staff including employees, councillors, agency staff, contractors, volunteers or any other persons who have access to, or use the Council’s information.

It covers:

- Requests from the public (FOI, EIR).
- Data Protection and privacy rights (UK GDPR & Data Protection Act).

3. Principles

Transparency

- The Council will be transparent about its information holding and processes.
- Privacy Notices will be made available to individuals.

Access to information

- The Council will respond promptly to requests for information under FOI and EIR.
- Requests for personal data will be handled in accordance with the UK GDPR and the Data Protection Act.

4. Collection, Use and Retention of Information

The Council collects information, including personal information, in order to operate as a local authority and to deliver services to members of the public. Where it is appropriate for information to be made publicly available, the Council will seek to do so by publishing it on its website and/or making it available by other means. In the case of some information, it will not be appropriate to share the information publicly e.g. where the information is confidential and/or there is a right to privacy.

In accordance with the legislation, the Council will only retain information for as long as necessary and will ensure that all information is held with appropriate levels of security. The Council maintains a retention schedule that sets out how long we will keep each type of information for.

5. Personal Information

The Council processes personal data only where necessary, proportionate and the requirements of data protection legislation are met. It handles all personal data in accordance with its Data Protection Policy.

Individuals that the Council holds personal data about have the following rights:

- The right to be informed about how and why their data is being used.
- The right of access to their own personal information held by the Council.
- The right of rectification where their data is inaccurate or not up to date.
- The right to erasure of their data.
- The right to restrict the processing of their data by the Council.
- The right to object to processing of their data by the Council.
- The right to have their data 'ported' to another organisation.
- Rights in relation to automated decision making and profiling.

The rights of individuals in relation to their personal data will depend on the purposes for which the Council is processing that data, which are set out in the Council's privacy notice(s).

Requests in relation to data subject rights can be made via the Council's website and the Council will respond to such requests as soon as possible (and in any event within the relevant timescales). Sometimes we may need to extend the timeframe for response where the request is large and/or complex, in which case we will advise the requestor as soon as possible. In some cases, we may ask the requestor to clarify or refine their request to enable us to provide an appropriate response.

We will endeavour to provide any information in the format requested, where it is reasonable and practicable to do so.

6. Other Information

The Council holds a range of information that any member of the public can submit a request to obtain a copy of, under either the Freedom of Information Act 2000 or the Environmental Information Regulations 2004 (or both). Information requests for such information can be made via the Council's website.

Where reasonable and practical to do so, we will make information publicly available on the Council's website or by other means.

If there are any charges or restrictions on use in relation to the information requested, then the requestor will be notified accordingly.

The Council will seek to respond to requests for information as soon as possible but in any event within the statutory timescales. Should there be a need to extend a deadline for any reason, the requestor will be notified.

Where a requestor is dissatisfied with the outcome of their request, it is open to them to request an internal review. Internal reviews will be carried out by another member of staff, independent to the officer that provided the initial response.

A requestor has the right to complain the Information Commissioner's Office if they remain

dissatisfied with the outcome following an internal review.

7. Relevant Legislation

The following legislation is relevant to this policy:

- The UK General Data Protection Regulation
 - Data Protection Act 2018
 - Human Rights Act 1998
 - Freedom of Information Act 2000
 - Environmental Information Regulations 2004
 - Local Government Acts
8. This Policy will be updated and or amended as necessary to reflect the changes in legislation and best practice.

Completion of Equality Impact Assessment (EIA) Form

Has an EIA form been completed as part of creating / reviewing / amending this policy?	Please tick: Yes <input checked="" type="checkbox"/> No <input type="checkbox"/>
If yes, where can a copy of the EIA form be found?	Available upon request
If no, please confirm why an EIA was not required?	



Records Management Policy

Item	Details
Reference:	Information Governance -1-RMP
Status:	Draft
Originator:	Head of Legal & Support Services
Owner:	Data Protection Officer
Version No:	1:1
Date:	[To be inserted once approved and published]

Key policy details

Approvals

Item	Date of Approval	Version No.
Consulted with N/A		
Reviewed by Audit and Governance Committee	7 August 2024	1:1
Approved by Cabinet	24 September 2024	1:1

The policy owner has the authority to make the following minor changes without approval.

Operational Changes - any modification in data protection procedures or required alignments with other documents within the Information Governance Framework.

Regulatory Decisions - when Court or regulatory decisions impact information security practices.

Guidance Changes - If there are changes in regulatory guidance related to data protection the policy owner should review and update this policy accordingly.

Policy Location

This policy can be found on the Council's website and on the Sharepoint page under current policies tab.

Revision History

Version Control	Revision Date	Summary of Changes
1:1	July 2024	Creation of Document

Policy Review Plans

This policy is subject to a scheduled review once every year or earlier if there is a change in legislation or local policy that requires it.

Distribution

Title	Date of Issue	Version No.
Distributed to Cabinet	24 September 2024	1:1
Published on NWLDC Website	TBC	1:1

Records Management Policy

1. Introduction

North West Leicestershire District Council's ("The Council") records support effective service delivery, provide evidence of its activities and decisions, and maintains the corporate memory. It is important that the Council manages its records appropriately to ensure that it complies with data protection legislation and is able to locate information when required. Systematic management of records protects the Council's most important information and improves business resilience and efficiency.

This policy establishes guidelines for the management, retention and disposal of data records within the Council. It sets out the Council's lifecycle approach to records management and the expectations for all employees in managing information effectively.

2. Scope

This policy forms part of the Council's Information Governance Framework, which applies to all staff including employees, councillors, agency staff, contractors, volunteers or any other persons who have access to, or use the Council's information.

This policy applies to all records that the Council holds, including the following:

- Documents (including hand-written, typed, and annotated copies).
- Paper based files.
- Computer files (including word processed documents, databases, spreadsheets and presentations).
- Maps and plans.
- Electronic mail messages (email).
- Web pages (on either the intranet and internet).
- Faxes.
- Brochures and reports.
- Forms.
- Audio and video tapes including CCTV and voicemail / voice recording systems.

3. Use

All information must be used consistently, only for the intentions for which it was intended and never for an individual employee's personal gain or purpose. If in doubt employees should seek guidance from the Data Protection Officer.

Disclosure - only specific information required should be disclosed to authorised parties and always in accordance and with strict adherence to the Data Protection Act. There are a range of statutory provisions that limit, prohibit or set conditions in respect of the disclosure of records to third parties and similarly arrange of provisions that require or permit disclosure.

3.1 Storage of Records

There is an Information Asset Register/ Record of Processing Activities.

The Council has an Information Asset Register/ Record of Processing Activities that identifies the assets owned by the Council and location of the same. It is subject to annual review and any risk found will be reported to the SIRO.

3.2 Retention

The retention period varies dependant on the type of information being stored. All Council Records retention periods should be detailed in the Information Asset Register and can be checked in the Corporate Retention Schedule available as part of the Council's Information Governance Framework.

The information must be relevant, fit for purpose it was intended and only retained for as long as it is genuinely required.

3.3 Disposal - It is particularly important under Data Protection legislation that the disposal of records, which is defined as the point in their lifecycle when they are either transferred to an archive or destroyed, is undertaken in accordance with clearly established policies which have been formally adopted by the Council.

3.4 Transfer - The mechanisms for transferring information from one organisation to another should be tailored to the sensitivity of the material contained within the records and the media on which they are held. The DPO can advise on appropriate safeguards.

4. Relevant Legislation

The Council is committed to continuously improving the way it responds to information requests that fall under specific statutory regimes.

The UK General Data Protection Regulation
The Data Protection Act 2018
The Freedom of Information Act 2000
The Environmental Information Regulations 2004

The following legislation is also relevant to this policy:

- Human Rights Act 1998
- The Local Government (Records) Act 1962 - this gave Local Authorities limited discretionary power to hold their records in local archives
- The Local Government Act 1972 - sets out the basic requirement for local authorities to 'make proper arrangements' to keep good records

5. Information Management Framework

NWLDC has implemented a framework of processes, procedures, standards and training materials together with defined roles and responsibilities that has been established, in order to support compliance with this policy so that:

- i) Appropriate information and documents are captured as records;
- ii) Records can be easily accessed by those who need them;
- iii) Records are available for as long as they are required in accordance with legislation and listed;
- iv) Records are disposed of appropriately when no longer required in line with legal and regulatory obligations;
- v) Records will be appropriately marked and kept securely and protected from accidental loss or destruction.

6. Roles And Responsibilities

The Senior Information Risk Owner (SIRO)

The Council has appointed the Monitoring Officer as the SIRO. The SIRO has responsibility for ensuring that effective systems and processes are in place to address the Information Governance agenda.

The SIRO is the overall owner of the information risk within the Council and acts as the focal point for information risk management within the Council including resolution of any risk issues raised by IAO. The SIRO will report annually to the Audit and Governance Committee on the content of the SIRO Report regarding information risks.

Information Asset Owners (IAO)

Each information Asset will have a relevant team manager as an Information Asset Owner.

The information asset includes records associated with the operation of the directorate function. Key decisions about the management of information will be made by the IAO. IAO provide quarterly assurances to the SIRO detailing any information asset records) perceived to be at risk

Data Protection Officer (DPO)

The DPO appointed under statutory GDPR obligations, is responsible for monitoring the Council's compliance with data protection legislation and its compliance with its own policies in relation to the protection of personal data. Monitoring of this policy will be overseen by the DPO. In the event of identification of high risks, the DPO will escalate to the appropriate level of management.

All Staff

All Council employees are responsible for any records that they create or use in the course of their duties. It is the responsibility of all employees to adhere to this policy when handling all types of Council information.

Equality Analysis

Completion of Equality Impact Assessment (EIA) Form

Has an EIA form been completed as part of creating / reviewing / amending this policy?	Please tick: Yes <input checked="" type="checkbox"/> No <input type="checkbox"/>
If yes, where can a copy of the EIA form be found?	Available upon request
If no, please confirm why an EIA was not required?	