



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, 22 July 2020
Location	Remote meeting using Microsoft Teams
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 disclosable interests you should make clear the nature of that interest and whether it is pecuniary or non-pecuniary.	
3. MINUTES	
To confirm and sign the minutes of the meeting held on 17 March 2020	3 - 6
4. INTERNAL AUDIT PROGRESS REPORT	
Report of the Audit Manager	7 - 22
5. INTERNAL AUDIT ANNUAL REPORT	
Report of the Audit Manager	23 - 32
6. TREASURY MANAGEMENT STEWARDSHIP REPORT 2019/20	
Report of the Finance Team Manager	33 - 46
7. PROGRESS OF IMPROVEMENTS IDENTIFIED THROUGH ANNUAL GOVERNANCE REVIEW 2018/19	
Report of the Head of Finance	47 - 52
8. REVIEW OF CORPORATE POLICIES	
Report of the Head of Finance	53 - 208

9.	STANDARDS AND ETHICS - QUARTER 3 REPORT	
	Report of the Head of Legal and Commercial Services	209 - 218
10.	STANDARDS AND ETHICS - QUARTER 4 REPORT	
	Report of the Head of Legal and Commercial Services	219 - 228
11.	STANDARDS AND ETHICS - QUARTER 1 REPORT	
	Report of the Head of Legal and Commercial Services	229 - 238
12.	DRAFT MEMBER CONDUCT ANNUAL REPORT	
	Report of the Head of Legal and Commercial Services	239 - 248
13.	REVIEW OF THE MODEL CODE OF CONDUCT	
	Report of the Head of Legal and Commercial Services	249 - 252
14.	UPDATE OF THE COUNCIL'S CONSTITUTION	
	Report of the Head of Legal and Commercial Services	253 - 258
15.	COMMITTEE WORK PLAN	
	To note the Committee's work plan	259 - 260

Circulation:

Councillor S Gillard (Chairman)
 Councillor D Harrison (Deputy Chairman)
 Councillor C C Benfield
 Councillor D Bigby
 Councillor J Clarke
 Councillor M D Hay
 Councillor K Merrie MBE
 Councillor V Richichi
 Councillor S Sheahan
 Councillor M B Wyatt

MINUTES of a meeting of the AUDIT AND GOVERNANCE COMMITTEE held in the Council Chamber, Council Offices, Coalville on TUESDAY, 17 MARCH 2020

Present:

Councillors D Bigby, S Gillard, M D Hay and S Sheahan

In Attendance: Councillors T Gillard and R Johnson

Officers: Mrs T Bingham, Miss E Warhurst, Mr T Delaney and Mrs R Wallace

External Audit: Mr M Surridge

31. ELECTION OF CHAIRMAN

It was proposed by Councillor D Bigby, seconded by Councillor S Gillard and

RESOLVED THAT:

Councillor S Sheahan take the chair for the remainder of the meeting.

32. APOLOGIES FOR ABSENCE

Apologies for absence were received from Councillors V Richichi, D Harrison, C Benfield, J Clarke, L Gillard and M Wyatt.

33. DECLARATION OF INTERESTS

There were none.

34. MINUTES

Consideration was given to the minutes of the meeting held on 4 December 2019.

It was moved by Councillor D Bigby, seconded by Councillor S Sheahan and

RESOLVED THAT:

The minutes of the meeting held on 4 December 2019 be approved as a correct record and signed by the Chairman.

35. INTERNAL AUDIT PROGRESS REPORT

The Head of Legal and Commercial Services presented the report.

In response to questions from Councillor D Bigby, the Head of Finance confirmed the position on small capital items, wider asset disposal policy as outlined in Appendix C of the report. She also confirmed a report addressing the issue would be going to Corporate Scrutiny Committee at a later date.

It was also confirmed that a response to a question on Health and Safety arrangements as set out in Appendix D would be communicated to all Members by the Head of Human Resources and Organisational Development after the meeting.

It was proposed by Councillor S Gillard, seconded by Councillor D Bigby and

RESOLVED THAT:

The report be noted.

36. INTERNAL AUDIT ANNUAL PLAN

The Head of Legal and Commercial Services presented the report. She also stated that a Draft Internal Audit Annual Plan had been presented to a meeting of the Committee on 2 March to which attendance had been high and no objections to the plan has been raised.

Councillors D Bigby and S Sheahan expressed several concerns on whether the recent meeting to review the Draft Annual Plan had been a valuable exercise and questioned whether the objective of reviewing the plan could have been achieved without a meeting of the Committee.

In response to these queries, the Head of Legal and Commercial Services stated that the involvement of Members in reviewing the Annual Plan was important and observed that Members had requested greater involvement in previous years. There was also a commitment to review the methods of communication and involvement for future meetings.

It was proposed by Councillor D Bigby, seconded by Councillor S Gillard and

RESOLVED THAT:

A) The committee notes the report and comments as appropriate
The Committee approves the 2020/21 Internal Audit Annual Plan

37. ANNUAL REPORT ON GRANTS AND CLAIMS

The Head of Finance presented the report.

It was proposed by Councillor D Bigby, seconded by Councillor M Hay

RESOLVED THAT:

The Committee notes the Section 151 Officer's update on Grants and Claims for the 2018/2019 year

38. EXTERNAL AUDIT PLAN

The Head of Finance presented the report with the aid of the External Auditor from Mazaars who attended the meeting virtually.

In response to a question from Councillor S Sheahan, the External Auditor provided further information around the plans to address the risks with regard to property, plant and equipment valuation as set out on page 11 of the report.

It was moved by Councillor D Bigby, seconded by Councillor M Hay and

RESOLVED THAT:

The Committee note the External Audit Plan for 2019/20

39. ACCOUNTING POLICIES AND MATERIALITY 2019/20

The Head of Finance presented the report.

It was observed that since this report had been first suggested two years ago it had become an important item on the Committee's agenda and very helpful in forming annual accounts.

It was proposed by Councillor S Gillard, seconded by Councillor D Bigby and

RESOLVED THAT:

- A) The Draft Accounting policies for the 2019/20 Financial statements as detailed in Appendix A be approved
- B) The Materiality Limits as set out in Appendix B be approved

40. CORPORATE RISK UPDATE

The Head of Finance presented the report. She highlighted that the risk was local government reorganisation was a growing risk with the upcoming Devolution White Paper from government and the potential for an East Midlands Combined Authority.

The Head of Finance added that since the report had been written the risk of unplanned vacancies had risen due to the national outbreak of Covid-19. The Committee was also informed that all Members would be receiving communication from the Chief Executive in the coming days setting out the Council's responses and actions going forward with regard to Covid-19.

In response to a question from Councillor D Bigby, the Head of Finance clarified the criteria used to determine the Movement of Risk as set out in the report and the reasoning behind several of the assessments. She acknowledged that there was room for improvement to make the determination clearer.

In response to a question from Councillor Sheahan, the Head of Finance confirmed that the risks associated with a 'no deal' Brexit had remained static whilst government negotiations on a future relationship were ongoing.

Councillors Sheahan and Bigby raised several concerns on the potential impacts of the Covid-19 outbreak and what measures the Council was undertaking to address the issue.

In response, the Head of Finance and the Head of Legal and Commercial Services confirmed that the Council was implementing existing emergency plans. It was also reiterated that all members would be receiving further communication from the Chief Executive in the coming days.

Councillor Sheahan acknowledged this response. On behalf of the Committee, he also stated that he was highly appreciative of the efforts being taken by Officers behind the scenes to ensure Council services remained operational.

It was proposed by Councillor D Bigby, seconded by Councillor S Gillard and

RESOLVED THAT:

The Quarter 3 Corporate Risk Update be noted

41. COMMITTEE WORK PLAN

A discussion was held at the beginning of the meeting with regard to the current outbreak of Covid-19 nationally and the need to restrict the business of the Committee

RESOLVED THAT:

The item be deferred until the next meeting of the Committee

The meeting commenced at 6.30 pm

The Chairman closed the meeting at 7.06 pm

NORTH WEST LEICESTERSHIRE DISTRICT COUNCIL

AUDIT AND GOVERNANCE COMMITTEE – WEDNESDAY, 22 JULY 2020



Title of Report	INTERNAL AUDIT PROGRESS REPORT	
Presented by	Lisa Marron Audit Manager	
Background Papers	Public Sector Internal Audit Standards Internal Audit Plan 2020/21	Public Report: Yes
Purpose of Report	To inform the Committee of progress against the Internal Audit plan for 2020/21 and to highlight any incidences of significant control failings or weaknesses that have been identified.	
Recommendations	THE AUDIT AND GOVERNANCE COMMITTEE NOTE THE REPORT.	

1.0 BACKGROUND

- 1.1 The Public Sector Internal Audit Standards require the Authority's Audit Committee to approve the audit plan and monitor progress against it. The Standards state that the Committee should receive periodic reports on the work of internal audit.
- 1.2 The Audit and Governance Committee approved the 2020/21 Audit Plan on 17 March 2020. The Committee receives quarterly progress reports.

2.0 PROGRESS REPORT

- 2.1 The Internal Audit Progress Report for the period 01 April 2020 to 30 June 2020 (Q1) is attached at Appendix 1.

Policies and other considerations	
Council Priorities:	An effective internal audit service supports all council priorities.
Policy Considerations:	None.
Safeguarding:	None.
Equalities/Diversity:	None.
Customer Impact:	None.
Economic and Social Impact:	None.
Environment and Climate Change:	None.
Consultation/Community Engagement:	None.
Risks:	There are no specific risks associated with this report.
Officer Contact	<p>Lisa Marron Audit Manager Lisa.marron@nwleicestershire.gov.uk</p> <p>Elizabeth Warhurst Head of Legal and Commercial Services elizabeth.warhurst@nwleicestershire.gov.uk</p>



INTERNAL AUDIT SHARED SERVICE

North West Leicestershire District Council

Internal Audit Progress Report 2020/21 Q1

1. Introduction

- 1.1 Internal Audit is provided through a shared service arrangement by North West Leicestershire District 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 2020/21 Internal Audit Plan up to 30th June 2020.

2 Internal Audit Team Update

- 2.1 Due to the Covid-19 it was agreed to not start working on the 2020/21 plan and instead Internal Audit team work has focussed on:
- Completing the 19/20 audit plan.
 - Providing advisory support.
 - Redeployment to support Covid-19 Business Grants work.
 - Aligning shared internal audit service approach and documents.

3 Internal Audit Plan Update

- 3.1 Work has not yet commenced on the 2020/21 Plan, details of which can be found at Appendix A. The Audit Manager is liaising with CLT to review the original plan in light of the significant changes to services in response to the pandemic, to establish:
- Audits that are no longer considered to be high risk or service suspension/staff redeployment means that the audit would not add value as planned.
 - New areas for the 2020/21 plan following significant changes to ways of working.
 - Audits that can proceed as planned.
- 3.3 Since the last update report three final audit reports for 2019/20 have been issued and the executive summaries for these are included in Appendix B.

4 Internal Audit Recommendations

- 4.1 Internal Audit monitor and follow up all critical, high and medium priority recommendations. All ongoing Internal Audit recommendations are included in Appendix C for information, as well as recommendations that have been made and implemented during Q1 to show progress.
- 4.2 It is noted that a number of recommendations due to be implemented have been delayed due to the impact of Covid-19 on the individual services. The Audit Manager does not have any concerns to highlight at this time.

5 Internal Audit Performance Indicators

- 5.1 Progress against the agreed Internal Audit performance targets are documented in Appendix D. There are no areas of concern at this stage however it is recognised that the 2020/21 plan will need to be reviewed to ensure it remains risk based following the significant changes to services in response to the pandemic.

Appendix A

2020/21 AUDIT PLAN

AUDIT AREA	TYPE	TIMING	COUNCIL PRIORITY AREA	PLANNED AUDIT DAYS
HR & ORGANISATIONAL DEVELOPMENT				
Health & Safety	Audit	Q3	2	3*
Project Management	Advisory	As required	All	3
			Subtotal	6
HOUSING AND PROPERTY				
Key Housing Systems	Audit	Q3/4	3	20
New Housing System Data Validation	Assurance	Q1	3	3
Gas Repairs and Maintenance Contract	Audit	Q3	3	6
Fire Safety and Management	Audit	Q2	3	8
			Subtotal	37
COMMUNITY SERVICES				
Grounds Maintenance	Audit	Q3	5	6
Waste Services	Audit	Q2/3	5	8
CCTV	Audit	Q2	2	5
Fleet Management	Audit	Q2/3	5	8
Safeguarding	Audit	Q1	2	6
			Subtotal	33
FINANCE				
CIPFA Financial Management Code	Audit	Q2	All	6
Key financial systems	Risk Based	Q3/4	All	30
Insurance	Advisory	As required	All	1

			Subtotal	37
CUSTOMER SERVICES				
Central Control	Audit	Q2/3	2	6
Customer Services	Audit	Q2/3	2	6
*as will be buying in			Subtotal	12
			Total	125

Appendix B

EXECUTIVE SUMMARY OF FINAL AUDIT REPORTS ISSUED SINCE LAST UPDATE REPORT

Report	Portfolio Holder(s)	Head of Service & Team Manager	Assurance Level	Areas for Improvement	Recommendations				
					C*	H	M	L	A
2019/20 Audit									
Affordable Housing – S106/Commutated Sums (11)	Housing, Property and Customer Services	Head of Housing Housing Strategy and Systems Team Manager Head of Planning and Infrastructure Planning Policy Team Manager	Grade 2	Formal agreement to the basis for calculation of commuted sums. Processes and authorisations for agreement of the value of commuted sums in lieu of affordable housing and funding of developments using these monies.	-	2	4	-	-
Planning Enforcement (13)	Community Services	Head of Community Services Environmental Protection Team Manager	Grade 1	Consistency in recording and uploading information to case records.	-	-	1	-	-
Commercial Lettings (14)	Housing, Property and Customer Services	Head of Customer Services, Corporate Property and Assets Property Services Manager	Grade 1	Carrying out rent reviews. Requesting of evidence (where applicable) from tenants to confirm they are complying with their responsibilities in accordance with the lease agreement.	-	1	1	-	1

KEY

Audit Opinion 2019/20

Grade	Definition
1	Internal Controls are adequate in all important aspects
2	Internal Controls require improvement in some areas
3	Internal Controls require significant improvement

4	Internal Controls are inadequate in all important aspects
---	---

Recommendation Priority

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	Recommendations concerning issues which are considered to be of a minor nature, but which nevertheless need to be addressed.
Advisory	Issues concerning potential opportunities for management to improve the operational efficiency and/or effectiveness of the system.

Appendix C

RECOMMENDATIONS TRACKER – ONGOING RECOMMENDATIONS (CRITICAL, HIGH AND MEDIUM ONLY)

Report		Recommendation	Rating	Officer Responsible	Target Date	Internal Audit Comments
2018/19 Audits						
7	Health and Safety	6	The role of the Safety Officer should be reviewed and a benchmarking exercise undertaken to determine the level of resource and responsibilities in this area at other Councils. Where the current resource is found to be insufficient to meet requirements the need for additional resource should be explored.	High	Head of HR & OD	<p>Jul 19</p> <p>March 2020 further extended to August due to Covid-19.</p> <p>Partly implemented.</p> <p>The Safety Officer has obtained details of staff with H & S roles similar to his at neighbouring authorities and passed this information to the Head of HR and Organisational Development. He will then review the resource commitment when the exact requirements of the role are known following the changes to systems and processes and the work of the task and finish group has been further progressed. This has been delayed due to Covid-19.</p>
15	New Council Houses	4	The corporate strategy to cover the supply of new affordable housing should be finalised and submitted to the Newbuild Group and CLT and should include all relevant opportunities i.e. new builds, gifted properties and those purchased directly from developers, long-term	Medium	Head of Housing/ Strategy and Systems Team Manager	<p>31.10.19</p> <p>31.03.20</p> <p>Update provided by Head of Housing: Draft New Supply Strategy produced by the Strategy and Systems Team Manager in 2019 has been reviewed and is currently being amended. It will become an interim Housing Strategy as the existing one expires in 2020 and the current situation prevents a full new strategy from being developed and delivered. Post Covid-19 a new timetable will be determined to update the full Housing Strategy to complement the Local Plan review</p>

			empty properties and those previously purchased by tenants under the Right to Buy Scheme and then offered back to the Council.				<p>timetable. The timetable for approval of the New Supply Strategy is -</p> <ul style="list-style-type: none"> • Final draft strategy completed – 30 June 2020 • Stakeholder consultation July/August 2020 • Corporate Scrutiny – 2 September 2020 • Cabinet – 22 September 2020
		5	Formal performance reports in respect of the key areas of the new build project should be provided to CLT at regular intervals.	Medium	Head of Housing	In line with corporate project reporting timetable	<p>Update provided by Head of Housing:</p> <p>Formal performance monitoring of new build/new supply project delivery will be incorporated into the refocused post Covid-19 project governance structure of the Council. In the interim performance will continue to be monitored through the bi-monthly New Supply Project Team meetings and the strategic New Supply Group, chaired by the Strategic Director with the Head of Housing and Housing Finance Manager. Reporting is then by exception to CLT, and regular progress reporting to Members via the quarterly performance monitoring reports to Scrutiny and Cabinet. Portfolio and shadow portfolio holder briefings are held monthly and cover new build and new supply progress updates.</p>
2019/20 Audits							
9	General Fund Assets	1	A single asset register should be maintained which contains all council assets. Each asset should have a unique reference number in order that it can be easily identified and responsibility for maintaining the asset	Medium	Finance Team Manager in conjunction with Property Services Manager	<p>31st May 2020</p> <p>30th Sept 2020</p>	Audit follow up in June 2020 established that recommendation has not be implemented due to Covid-19. Target date extended and new audit follow up date October 2020.

			register should be clearly assigned.				
10	Information Governance Arrangements	1	The Data Protection Officer (DPO) should work to develop a user friendly web page which contains information the Council is required to publish as part of the Local Transparency Code. Once developed the DPO should monitor the page to ensure that the information contained is up to date and prompt services to update information where required.	Medium	Data Protection Officer	31st Mar 2020 31 st August 2020	In progress however had to pause due to Covid-19.
11	Affordable Housing – S106/Commuted Sums	1	The guidance available on the Council website relating to Affordable Housing should be reviewed. Those documents which are out of date or no longer relevant should be removed.	Medium	Planning Policy Team Manager	31 st August 2020	Audit follow up September 2020.
		2	The completion of an Affordable Housing – Supplementary Planning Document (SPD) should be progressed. In the meantime it should be formally agreed that where a calculation is required to agree a commuted sum in lieu of affordable housing that	High	Planning Policy Team Manager	31 st August 2020	Audit follow up September 2020.

			the guidance in the 2011 SPD is referred to.				
		3	There should be a formal approval process in place to confirm agreement to the amount of commuted sum that is required in lieu of affordable housing. Details of how the sum has been arrived at and evidence to confirm this should be retained. Evidence that the approval process has been followed should accompany the request to Legal Services when preparing the S106 agreement.	High	Head of Planning & Infrastructure	31 st August 2020	Audit follow up September 2020.
		4	The forms required to be completed when requesting release of S106 affordable housing commuted sums should be reviewed to ensure they are relevant and up to date. Consideration should be given to including a section for finance to complete prior to the authorisation section to complete any appropriate checks for example confirmation that the amounts have not be committed elsewhere. Once	Medium	Affordable Housing Enabling Officer	31 st August 2020	Audit follow up Sep-20

			updated and agreed the forms should be made available on SharePoint.				
		5	Those officers responsible for authorising release of commuted sums should be reviewed and confirmed.	Medium	Head of Planning & Infrastructure and Head of Housing	31 st August 2020	Audit follow up Sep-20
		6	The priorities for the use of commuted sums should be reviewed and agreed formally, if necessary, to ensure clarity and transparency.	Medium	Housing Strategy and Systems Team Manager	31 st August 2020	Audit follow up Sep-20
12	Planning Enforcement	1	Guidance should be issued to Enforcement Officers regarding cases where HARM scores are required to be completed. This guidance should also include details of documentation which would be expected to be uploaded to and the fields required to be completed in Uniform.	Medium	Senior Enforcement Officer	31 st May 2020	Implemented
13	Commercial Lettings	1	The service should review the procedures in place relating to Commercial Lettings. Where areas are identified that would benefit from there being written procedures in place these should be produced. As a priority	High	Property Officer	30 th Sep 2020	Audit follow up October 2020.

			this should include procedures for carrying out rent reviews to ensure these are reviewed on a timely basis.				
		2	Property Services should put in place a process whereby evidence is requested from tenants to confirm that they are complying with the terms of their lease agreement. Examples of this would be gas servicing / boiler maintenance, any relevant insurance etc.	Medium	Property Services Team Manager	30 th Sep 2020	Audit follow up October 2020.

Appendix D

2020/21 INTERNAL AUDIT PERFORMANCE

Performance Measure	Position as at 30.06.20	Comments
Achievement of the Internal Audit Plan	0%	Work not started on 2020/21 plan due to Covid-19 impact. Audit Manager currently liaising with Heads of Service.
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	Follow up testing up to date however some delays to implementation of recommendations due to Covid-19.
Annual Opinion Report - July 2020 Audit and Standards Committee Meeting	On track	
100% Customer Satisfaction with the Internal Audit Service	100%	Based on returns for 19/20.

This page is intentionally left blank

NORTH WEST LEICESTERSHIRE DISTRICT COUNCIL

AUDIT AND GOVERNANCE COMMITTEE – WEDNESDAY,
22 JULY 2020



Title of Report	INTERNAL AUDIT ANNUAL REPORT	
Presented by	Lisa Marron Audit Manager	
Background Papers	Public Sector Internal Audit Standards	Public Report: Yes
Purpose of Report	<p>To present the annual internal audit opinion on the overall adequacy and efficiency of the Council's framework of governance, risk management and control.</p> <p>This is required by the Public Sector Internal Audit Standards and should be used to inform the Annual Governance Statement.</p>	
Recommendations	THAT THE COMMITTEE NOTES THIS REPORT AND COMMENTS AS APPROPRIATE.	

Policies and other considerations, as appropriate	
Council Priorities:	An effective internal audit service and risk based plan supports all council priorities.
Consultation/Community Engagement:	The Head of Legal and Commercial Services has been consulted.
Risks:	Not presenting this report to Committee would mean that we have not complied with the Public Sector Internal Audit Standards.
Officer Contact	Lisa Marron Audit Manager lisa.marron@nwleicestershire.gov.uk



INTERNAL AUDIT SHARED SERVICE

North West Leicestershire District Council

Internal Audit Annual Report 2019/20

1. 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 2019 to 31 March 2020 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.
- 1.3 This report also includes:
- A summary of internal audit work carried out during 2019/20 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 2019/20

- 2.1 I am satisfied that sufficient internal audit work has been undertaken 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 and the most that Internal Audit can provide is reasonable assurance that there are no major weaknesses in the system of internal control.
- 2.2 For the 12 months ended 31 March 2020, I have formed the opinion that the Council's control environment is a **Grade 2** overall. To be consistent with our Internal Audit opinion grade definitions, this means that I consider that the control environment requires improvement in some areas. This is a positive assurance opinion overall.
- 2.3 My opinion is based on the following:
- All internal audit work undertaken during the year.
 - Follow up audit work in respect of audit recommendations.
 - My knowledge of the Council's governance and risk management structure and processes.
- 2.4 There have been no impairments to the independence of internal auditors during the year.

3. SUMMARY OF INTERNAL AUDIT WORK DURING 2019/20

- 3.1 The risk based internal audit plan for 2019/20 was presented and approved by the Audit and Governance Committee on 20th March 2019. The plan was developed to

provide assurance on the overall adequacy and effectiveness of internal controls, risk management and governance across a range of financial and organisational areas that were identified as part of the risk based planning process. Progress against the 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 2019/20 by the in-house team 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 original audit plan. The completion of the 2019/20 plan was not impacted by the Covid-19 pandemic.

In addition, an IT General Controls audit was provided by a specialist ICT auditor. The opinion for this audit was a Grade 1.

Table 1

Audit Opinion	Number
Grade 1 – Internal controls are adequate in all important aspects	10
Grade 2 – Internal controls require improvement in some areas	3
Grade 3 – Internal controls require significant improvement	0
Grade 4 – Internal controls are inadequate in all important aspects	0
Total	13

- 3.3 Internal Audit follow up progress against recommendations in line with the timescales agreed at the time of issuing reports. The 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 2019/20 is included at Appendix B.

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

- 4.1 All internal audit reports issued during 2019/20 were either a Grade 1 or a Grade 2.

A small number of high priority recommendations were made in respect of audit reviews undertaken, however as they relate to specific systems and/or service areas, I do not consider it necessary to include them in the Annual Governance Statement. The Section 151 Officer receives all Internal Audit reports issued therefore they are also able to make their own assessment when completing the Annual Governance Statement should they be of a different opinion.

5. QUALITY ASSURANCE AND IMPROVEMENT PROGRAMME (QAIP) FOR INTERNAL AUDIT

- 5.1 The Public Sector Internal Audit Standards (PSIAS) require the QAIP to include internal and external assessments (see Appendix C for more detail).
- 5.2 The internal assessments applicable to 2019/20 include the following:

- The Audit Manager planned all audit engagements and carried out documented reviews of working papers and draft reports prior to issue.
 - Monthly performance review meetings attended by the Audit Manager and the Head of Legal and Commercial Services as well as regular meetings with the Head of Finance.
 - Customer satisfaction surveys were sent out to all Heads of Service and Team Managers who had an audit in their service area. Eight returns for 2019/20 all with overall positive feedback.
 - Quarterly progress reports to senior management 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. Our external assessment was completed in April 2015 and the full report was presented to the Audit and Governance Committee meeting on 24th June 2015. The Audit Manager has made arrangements for the next external assessment to take place in November 2020 in order to allow all three partner authorities to be subject to the assessment.
- 5.4 In addition to delivering the annual audit plan and opinion, Internal Audit have added value in the following ways:
- Supporting a number of internal HR investigations to ensure that internal controls are robust with recommendations made to support improvements where appropriate.
 - Providing ad-hoc advice throughout the year to a wide range of services to help ensure that internal controls are maintained or strengthened.
 - Delivering a successful shared service to Blaby District Council which expanded to welcome Charnwood Borough Council from 1st April 2020. 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 April 2015 concluded that there were no significant gaps in compliance. The Standards were updated in April 2017 and the Audit Manager carried out a review against the additions to the Standards at that time to ensure that we remained compliant from April 2017. There have been no further updates to the standards during 2019/20.
- 6.2 I can confirm that during 2019/20 the Internal Audit Shared Service conformed to the Public Sector Internal Audit Standards.

Appendix A

RESULTS OF INDIVIDUAL AUDIT ASSIGNMENTS AGAINST THE 2019/20 AUDIT PLAN

Audit Area (report number)	Type	Planned Days	Actual Days	Status	Assurance Level	Recommendations					Comments
						C	H	M	L	A	
HR AND ORGANISATIONAL DEVELOPMENT											
Project Management	Audit	8	-	Defer to 2020/21.							Defer to 20/21 to allow new corporate arrangements to bed in.
Performance Management	Audit	6	-	Defer to 2020/21.							Defer to 2020/21 to allow full year of new system and final report to be included in audit.
4 –Expenses and Reimbursements	Audit	3	7	Final report issued.	Grade 2	-	1	2	2	1	
HOUSING AND PROPERTY											
Stock Condition Database	Audit	6	0.9	Removed from plan.							Housing Quality Network carrying out a piece of work on this area.
11 - Affordable Housing Section 106/Commutated Sums	Audit	6	10	Final report issued	Grade 2	-	2	4	-	-	
1 - New Housing System (Aareon) Implementation Project	Assurance	4	3.8	Final report issued.	Grade 1	-	-	-	-	-	
14 - Commercial Lettings	Audit	6	8	Final report issued.	Grade 1	-	1	1	-	-	
7 - Homelessness	Additional Audit	6	8.3	Final report issued.	Grade 2	-	3	2	-	-	
COMMUNITY SERVICES											
13 - Planning	Audit	6	7	Final report	Grade 1	-	-	1	-	-	

Audit Area (report number)	Type	Planned Days	Actual Days	Status	Assurance Level	Recommendations					Comments
						C	H	M	L	A	
Enforcement				issued							
3 - Licensing	Audit	6	9.3	Final report issued.	Grade 1	-	-	3	1	-	
CCTV	Audit	5	-	Deferred to 2020/21.							CCTV will be in new location from Q1 20/21.
5 - Leisure Contract Procurement	Audit	8	10.8	Final Report Issued	Grade 1	-	-	-	-	-	
ECONOMIC DEVELOPMENT											
2 - Enterprising NWL Grants (Monitoring)	Audit	5	4	Final report issued.	Grade 1	-	-	1	-	1	
LEGAL AND COMMERCIAL SERVICES											
10 - Information Governance	Audit	6	6	Final report issued	Grade 1	-	-	1	-	-	
FINANCE											
Procurement	Audit	8	-	Removed from plan.							Interim arrangements in place while internal review is carried out.
Key Financial Systems	Risk Based Audits	35	25	6 - Cash and Bank final report issued.	Grade 1	-	-	1	-	-	
				9 - General Fund Assets final report issued	Grade 1	-	-	1	-	-	
				12 – Rent Accounting final report issued	Grade 1	-	-	-	-	-	
CUSTOMER SERVICES											
8 - IT General Controls	3rd Party Auditor	2	1.3	Final report issued	Grade 1	-	-	1	-	-	

Audit Area (report number)	Type	Planned Days	Actual Days	Status	Assurance Level	Recommendations					Comments
						C	H	M	L	A	
Revenues and Benefits – DWP Memorandum of Understanding	Audit	3	-	Removed from plan.							Reliance will be placed on the work of Partnership Auditors.

SUMMARY OF INTERNAL AUDIT RECOMMENDATIONS FOLLOW UP 2019/20

Internal Audit follow up progress against critical, high and medium priority recommendations in line with the timescales agreed at the time of issuing reports. Any overdue recommendations are highlighted to Audit and Governance Committee. The table below shows the progress against recommendations made by Internal Audit during 2019/20.

Recommendation Priority	Recommendations Made	Recommendations Implemented	Recommendations Outstanding (In Progress or Not Yet Due)
Critical	-	-	-
High	7	4	3
Medium	18	10	8
Total	25	14	11

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	Recommendations concerning issues which are considered to be of a minor nature, but which nevertheless need to be addressed.
Advisory	Issues concerning potential opportunities for management to improve the operational efficiency and/or effectiveness of the system.

Appendix C

QUALITY ASSURANCE AND IMPROVEMENT PROGRAMME 2019-20

Activity	PSIAS	Result/comments	Frequency
External Quality Assessment	1310	April 2015 Assessment - no significant gaps in compliance.	Every 5 years.
Annual Declaration of Interests	1130	Last forms completed April 2019. New form produced to incorporate Code of Ethics and Principles ready for April 2020.	Annual
Customer satisfaction surveys	1311	Eight responses for 2019/20. All positive overall. We are responding to feedback by reviewing format of reports to include more information to support positive findings.	After each audit
Performance indicators reported in progress reports	1311	Performance indicators included in all quarterly reports to senior management and Audit and Governance Committee.	Quarterly
Improvement actions/continuous improvement	1311	An internal action plan produced for 2019/20 detailing improvement actions which include new ways of circulating draft audit reports using mod.gov and introducing learning and development record for Internal Audit team.	Ongoing
Review of all audit engagements and reports	1311, 2340	All audit engagements and reports are reviewed by another auditor 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 Commercial Services.	Monthly
Annual review of internal audit charter	1000	September 2019 review only identified minor changes to job titles and organisation charts.	Annual
Performance and development review process for staff and training and development records.	1200	All review meetings with team have taken place and a new training and development form introduced to record all training and development from April 2019. Officers recording their CPD in line with their professional body requirements do not need to duplicate records.	Bi- annual review meetings

NORTH WEST LEICESTERSHIRE DISTRICT COUNCIL

AUDIT & GOVERNANCE COMMITTEE – WEDNESDAY,
22 JULY 2020

Title of Report	TREASURY MANAGEMENT STEWARDSHIP REPORT FOR 2019/20	
Presented by	Anna Wright Finance Team Manager & Deputy S151 Officer	
Background Papers	Capital Strategy 2019/20 – Council 26 February 2019 Treasury Management Strategy Statement 2019/20 and Prudential Indicators 2019/20 to 2021/22 – Council 26 February 2019 Treasury Management Activity Report April 2019 to January 2020 – Audit and Governance 17 March 2020 Investment Strategy – Service and Commercial 2019/20 – Council 26 February 2019 Budget and Council Tax 2019/20 – Council 26 February 2019	Public Report: Yes
Purpose of Report	To inform Members of the Council's Treasury Management activity undertaken for the financial year 2019/20.	
Recommendations	THAT MEMBERS APPROVE THIS REPORT.	

1.0 BACKGROUND

- 1.1 Treasury Management activity is underpinned by CIPFA's Code of Practice on Treasury Management ("the code"), which requires local authorities to produce Prudential Indicators and a Treasury Management Strategy Statement annually on the likely financing and Investment activity.
- 1.2 This report fulfils the council's legal obligation under the Local Government Act 2003, to have regard to both the CIPFA Code and the Ministry of Housing, Communities and Local Government (MHCLG) Investment Guidance
- 1.3 In 2019/20, council approved its Capital Strategy (included in the Budget and Council Tax report) and Treasury Management Strategy Statement, including the Borrowing Strategy, Debt Rescheduling Strategy, Annual Investment Policy and Strategy, Interest Apportionment Policy, Prudential Indicators and Annual Minimum Revenue Position Statement in its meeting on 26 February 2019.

- 1.4 Investing or borrowing activities expose the council to financial risks including the loss of invested funds and the revenue effect of changing interest rates. The successful identification, monitoring and control of risks are therefore central to the council's treasury management strategy.

2.0 THE U.K. ECONOMY AND OTHER FACTORS.

- 2.1 An economic update and Interest rate forecast has been provided by our Treasury Advisers (Arlingclose Ltd) and summarised below. A full update can be found at Appendix A
- CPI fell to 1.7% in February 2020, below the Bank of England's target of 2%.
 - The unemployment was 3.9% in the three months to January 2020, while the employment rate hit a record high of 76.5%
 - GDP growth in Q4 was reported as flat by the Office for national Statistics with annual rate growth remained below-trend at 1.1%.
 - The coronavirus which first appeared in China in December 2019, started spreading across the globe caused falls in financial markets not seen since the Global Financial Crisis.
 - The Bank of England held policy rates steady at 0.75% through most of 2019/20, but moved in March to cut rates to 0.25%, and then swiftly thereafter reduced further to the record low of 0.1%.
 - The UK government introduced a number of measures to help businesses and households impacted by a series of ever-tightening social restrictions, culminating in pretty much the entire lockdown of the UK.

3.0 THE COUNCIL'S TREASURY POSITION.

- 3.1 The council's current strategy is to use internal borrowing to reduce risk and keep interest costs low. The treasury management change over the financial year is shown below.

	Balance at 01/04/2019 £m	Net Movement £m	Balance at 31/03/2020 £m
Long term borrowing - HRA	£72.80	-£1.10	£71.70
Long term borrowing – General Fund	£8.40	£0.00	£8.40
Other long-term liabilities - HBBC	£0.10	£0.00	£0.10
Total Borrowing	£81.30	-£1.10	£80.20
Long term investments – greater than 1 year	£3.00	£0.00	£3.00
Short term investments – less than 1 year	£39.60	£0.10	£39.70
Pooled funds and externally managed investments*	£5.80	£2.20	£8.00
Total Investments	£48.40	£2.30	£50.70
Net debt	£32.90	-£3.40	£29.50

*Represents investments held in Money Market Funds

- 3.2 The annual repayments on two PWLB annuity loans taken out as part of the self-financing system of Council Housing in 2011/2012, are shown in the Net Movement column.
- 3.3 In 2019/20, the capacity for investment has increased by £2.3m. This can be affected by various factors including: increased income, contributions to/from reserves, setting aside

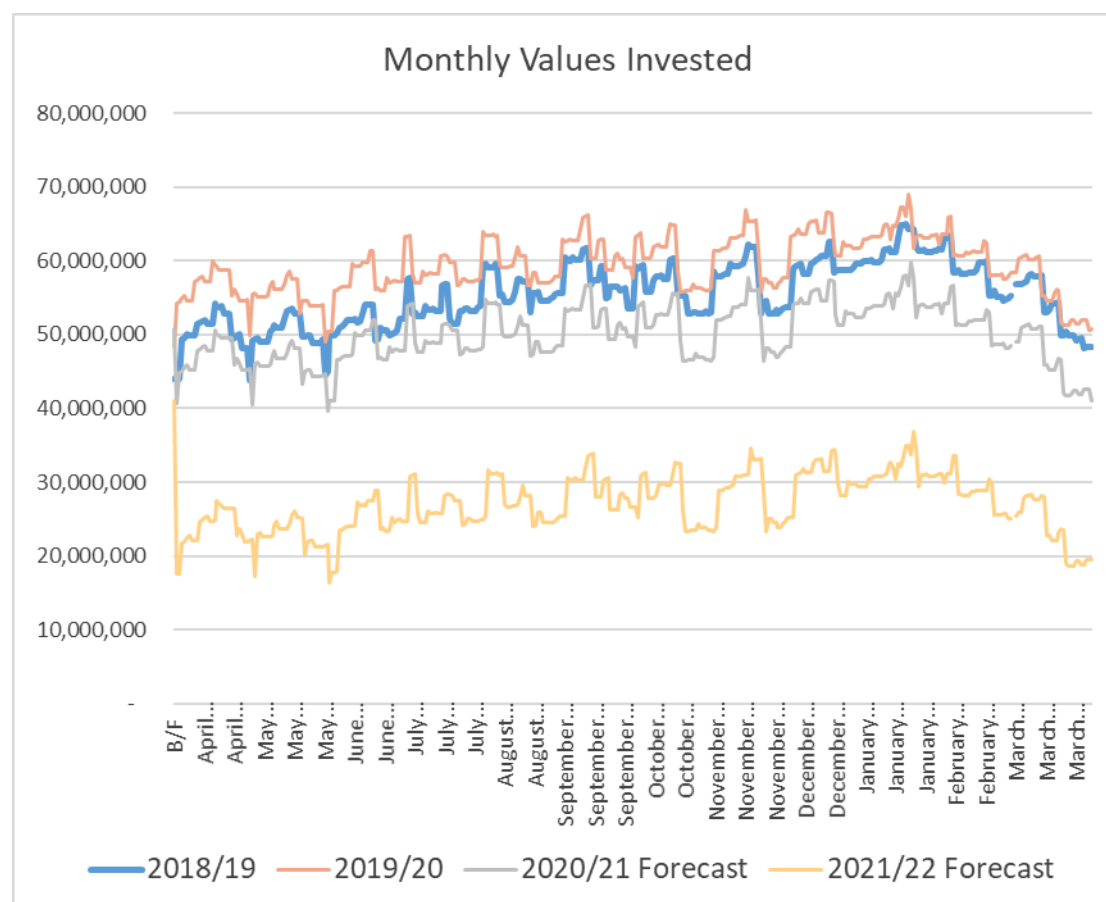
expenditure to repay borrowing (MRP), fortuitous income, cash flow timing of receipts and payments and internal borrowing.

3.4 In 2019/20, some of the highlights that have impacted on the capacity are:

- Sales of assets – circa £3.8m
 - General Fund Vehicles £11k
 - Housing Revenue Account
 - Land £950k
 - Council Houses RTB £3.562m
 - Council Houses Non RTB £210k
- MRP £618k
- Increased income from various activities across the council including: circa £193k from investment income and £30k re-cycling income.
- There was also a delay on implementation of 2019/20 Capital Programmes; General Fund £10.7m (largely attributable from the New Leisure Centre Project) and Housing Revenue Account for £2.8m.

3.5 The pattern of cash held and subsequently invested per day is shown in the chart below, illustrating the cash flow trends throughout the year. The delay in implementation of the New Leisure Centre Building for £7.3m was the main factor for the increased investment capacity in the year. This is expected to impact the Council's cash flow for 2020/21.

The chart below also shows the forecast position for 2020/21 and 2021/22. This reflects lower levels of cash available in the next two years since it is planned that internal borrowing will be used to fund Capital programmes along with the effect of the expected maturity of Housing Revenue Account's £13m PWLB loans in 2021/22.



4.0 BORROWING ACTIVITY.

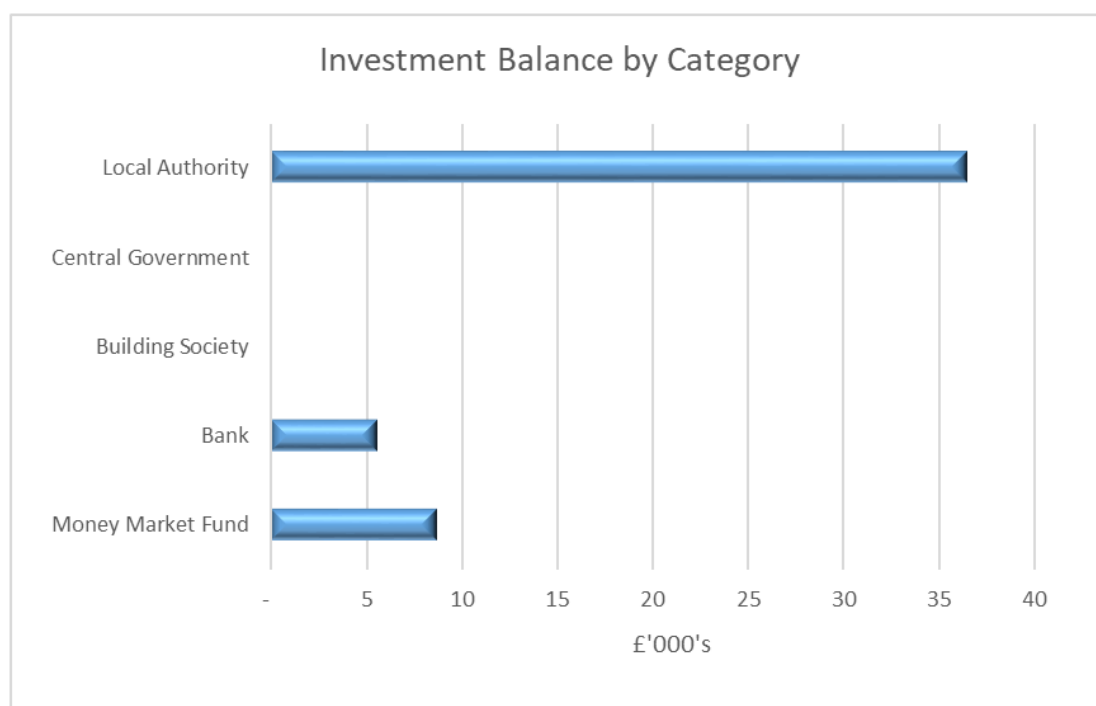
- 4.1 The council's Borrowing Strategy 2019/20, incorporates a prudent and pragmatic approach to borrowing to minimise borrowing costs without compromising the longer-term stability of the portfolio, consistent with the council's Prudential Indicators.
- 4.2 No loans matured in 2019/20 that required replacement.
- 4.3 The Borrowing Strategy identified that borrowing would not be required until 2020/21 and the council has not undertaken any new long-term borrowing during the year. Annual principal repayment of £1.1m and Interest payments totalling £2.71m were made in respect of existing debt. Members should note that a significant proportion of the HRA self-financing debt was taken out on a maturity basis and therefore whilst interest is paid, the principal repayment of the loan is not made. The Council has the funds set aside within HRA reserves for the first two maturity loan redemptions in 2022 of £3m and £10m, should it decide to repay the loans rather than refinance.
- 4.4 The council's cash flow remained positive and did not require and temporary loans during the year.
- 4.5 The council had approximately £9m of internal debt at 31 March 2020. This is the cumulative value of internal cash balances used to finance new capital expenditure instead of financing through unsupported borrowing. This is currently judged to be the most cost effective means of funding the capital programme.
- 4.6 The estimated Minimum Revenue Provision (MRP) is intended to ensure that the capital financing debt is paid off over the longer term. The MRP charge made to General Fund revenue account for 2019/20 is £618k.
- 4.7 The Housing Revenue Account is not required to make MRP charges. However, the council classes the principal repayments made in respect of the two PWLB annuity loans taken out as part of the housing self-financing in 2011/12, as MRP. In 2019/20, this repayment was £1.1m (as per 4.3 above).

5.0 DEBT RESCHEDULING ACTIVITY.

- 5.1 The council's Debt Rescheduling Strategy 2019/20, establishes a flexible approach where the rationale for rescheduling could be one or more of the following:
 - Savings in interest costs with minimal risk.
 - Balancing the volatility profile (i.e. the ratio of fixed to variable rate debt) of the debt portfolio.
 - Amending the profile of maturing debt to reduce any inherent refinancing risks.
- 5.2 No opportunities for debt rescheduling were identified which conformed to the above rationale. Accordingly, the council has undertaken no debt rescheduling activity during the year.
- 5.3 The council's portfolio of thirteen loans - ten PWLB loans and three market loans continue to be monitored for debt rescheduling opportunities.

6.0 TREASURY MANAGEMENT INVESTMENT ACTIVITY.

- 6.1 The main objective of the council's Investment Policy and Strategy 2019/20 is to invest its surplus funds prudently.
- 6.2 The council's investment priorities (S.L.Y.) are:
- **S**ecurity of the invested capital;
 - sufficient **L**iquidity to permit investments; and,
 - Optimum **Y**ield which is commensurate with security and liquidity.
- 6.3 To lower the inherent investment risk, the council has minimised the use of banks and increased the use of other Local Authorities as investment counterparties. A range of lengths of investment, from overnight investments to short and long fixed term, from 32 days to 3 years, are currently utilised to ensure that the principles of security, liquidity and yield are followed. The table below shows the range of counterparties used by the council and the values invested at 31 March 2020.



- 6.4 The counterparties that the council currently use all meet the criteria set out in the Treasury Management Strategy Statement 2019/20 and are monitored by the Treasury Management Advisors. A detailed list of the counterparties used and amounts currently invested can be seen in Appendix B.

Inter-Local Authority lending accounted for 68% of investments placed during the year. The Council's investments are made with reference to the Council's cash flow, the outlook for the UK Bank Rate, money market rates, the economic outlook and advice from the Council's treasury adviser.

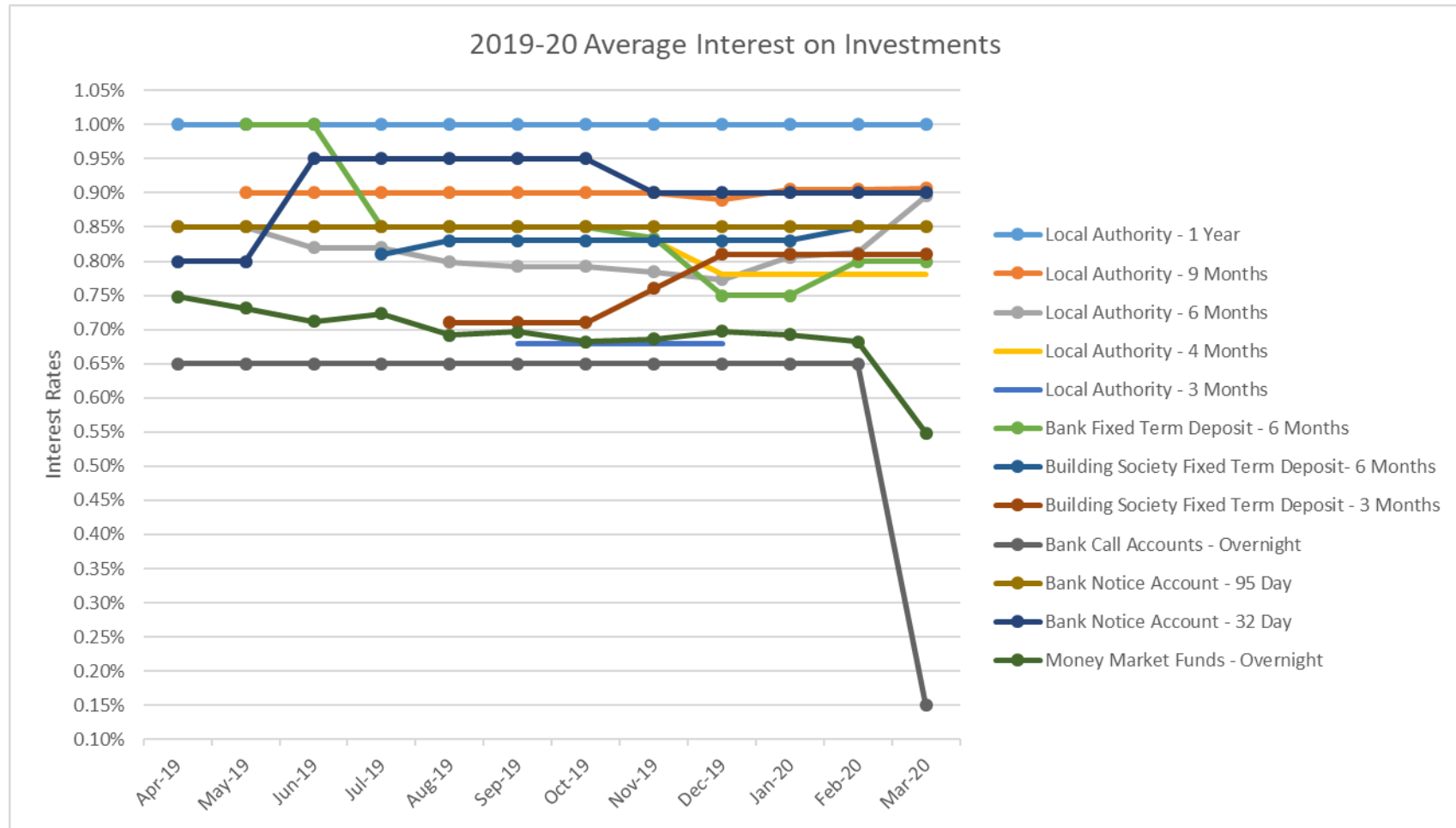
The Council exercises due diligence by assessing the organisation's financial stability. This is achieved by reviewing their credit status, most recent audited financial statements,

auditor's report, budget report and current news which is financial in nature. All decisions are signed off the by Section 151 Officer or her Deputy.

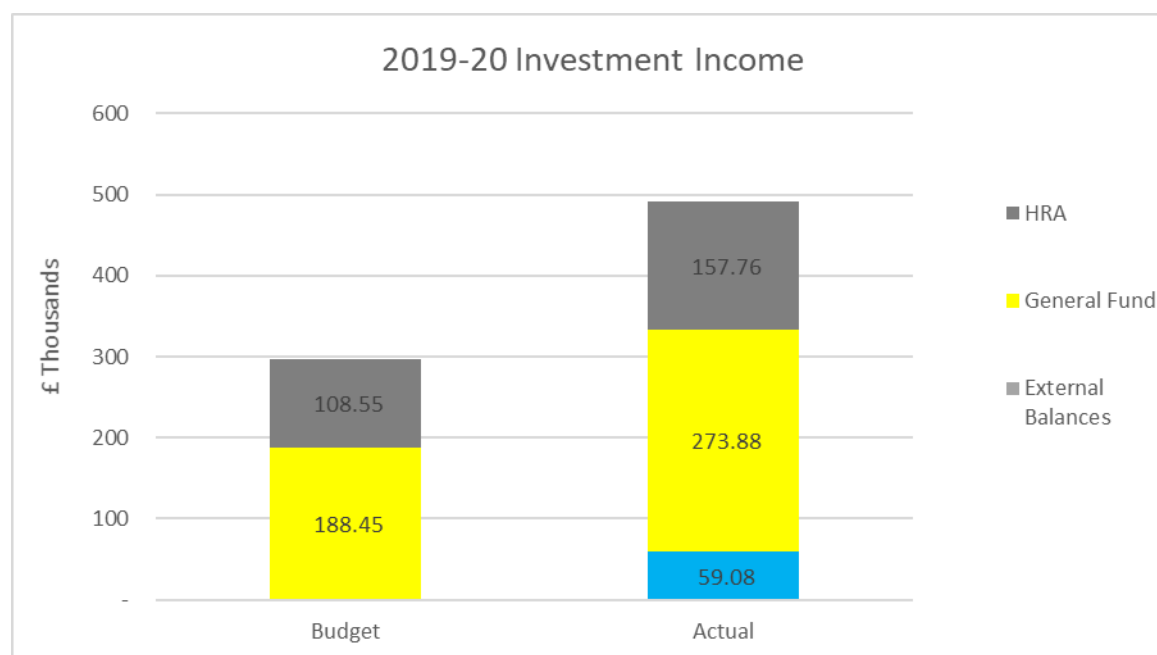
- 6.5 The average rate of return on the council's investment balances for the year was 0.82%. For comparison purposes, the benchmark return (average 7-day London Interbank Bid Rate or LIBID rate) on 31 March 2020 was 0.58% and the average 7 day London Interbank Offered Rate (LIBOR) rate was 0.58%. This shows that we are achieving a good rate of return against benchmark.
- 6.6 Paragraph 6.5 above explains that the current average rate of return of 0.82% has been achieved. This was an improved rate from the budgeted interest of 0.69% and contributed to the additional interest income of £193k above the budget of £297k.

The current COVID-19 pandemic has affected the financial market followed by the Bank of England cutting interest to as low as 0.10%. This resonated on interest rates across all investment opportunities and forecasted to be the same position for at least the remainder of the year. This is expected to dramatically reduce the interest income for the coming year which is budgeted at £260k based on an average interest rate of 0.68%.

The graph below shows the average interest rate on in year investments and the movement of interest rates over the year.



- 6.7 The council budgeted to achieve £297,000 of income from its investment activity in 2019/20 of which £188,450 is applied to General Fund and £108,550 to Housing Revenue Account. Investment activity for the year achieved £490,711 in interest.
- 6.8 Of the income achieved, an element is applied to balances held on external income. This external income largely represents balances from S106 contributions that have not yet been spent. The amount to be applied is £59,079. This is not budgeted for as S106 contributions are only achieved when specific conditions are met and are anticipated to be spent.
- 6.9 The remaining balance of £431,632 is apportioned between the General Fund which will receive £273,875; and Housing Revenue Account which will receive £157,756.
- 6.10 The budgeted and projected levels of investment income is represented in the table below.



- 6.11 There was one breach of investment limits in the year reported to Audit and Governance committee in December 2019. This was where the council went into an unapproved overdraft position. The council had a £1,000,000.00 deposit with Close Brothers at a rate of 1% for the period of 29 March 2019 to 30 September 2019. This trade was agreed through the broker on 28 March 2019. The funds were not credited in the Council's current bank account (as stated on the trade confirmation) on the 30 September 2019, or by 1 October 2019. The £1,000,000 deposit plus interest earned of £5,575.34 was received by the council on the 2 October 2019. This resulted in the council's bank account being overdrawn and bank charges incurred. The reason for the breach was that deal was repaid to another bank account. The overdraft charges and loss of 2 days interest has been fully reimbursed by Close Brothers Ltd.

7.0 NON-TREASURY INVESTMENT ACTIVITY

- 7.1 The definition of investments in CIPFA's revised Treasury Management Code now covers all the financial assets of the Authority as well as other non-financial assets which the Authority holds primarily for financial return. This is replicated in MHCLG's Investment Guidance, in which the definition of investments is further broadened to also include all such assets held partially for financial return.
- 7.2 The following list represents the council's current investments in this area.

Property or Type	Value at 31 Mar 2020	Reason held
Industrial Units	£6.5m	To support the local economy and to

		generate profits to supplement council expenditure
Markets	£1.5m	Any profit supplements council expenditure
Land	£4.8m	Future economic benefit

- 7.3 More detailed information can be found in the “Investment Strategy – Service and Commercial” which was presented to Council on 26 February 2019.
- 7.4 In November 2019, Cabinet approved a new Corporate Asset Management Strategy, which set out a framework from which to manage our corporate property assets for the next five years. This strategy commits to reviewing the financial performance of our commercial assets as a priority, and an external review identified an average yield of 7.88% across our portfolio. Lower yielding assets are planned to be reviewed as part of the Council’s Journey to Self Sufficiency programme to assess whether they can managed in a different way to increase overall portfolio yield.

8.0 SUMMARY

- 8.1 For the financial year 2019/20, the council can confirm that it has complied with its Prudential Indicators, which were approved as part of the council’s Treasury Management Strategy Statement.
- 8.2 The council can confirm that during the financial year, other than the breach of prescribed limit detailed in paragraph 6.12, it has complied with its Treasury Management Practices.

Economic information provided by Treasury Management Advisors

External Context *(based on data as at 24/04/20)*

Economic commentary

Economic background: The UK's exit from the European Union and future trading arrangements, had remained one of major influences on the UK economy and sentiment during 2019/20. The 29th March 2019 Brexit deadline was extended to 12th April, then to 31st October and finally to 31st January 2020. Politics played a major role in financial markets over the period as the UK's tenuous progress negotiating its exit from the European Union together with its future trading arrangements drove volatility, particularly in foreign exchange markets. The outcome of December's General Election removed a lot of the uncertainty and looked set to provide a 'bounce' to confidence and activity.

The headline rate of UK Consumer Price Inflation UK Consumer Price Inflation fell to 1.7% y/y in February, below the Bank of England's target of 2%. Labour market data remained positive. The ILO unemployment rate was 3.9% in the three months to January 2020 while the employment rate hit a record high of 76.5%. The average annual growth rate for pay excluding bonuses was 3.1% in January 2020 and the same when bonuses were included, providing some evidence that a shortage of labour had been supporting wages.

GDP growth in Q4 2019 was reported as flat by the Office for National Statistics and service sector growth slowed and production and construction activity contracted on the back of what at the time were concerns over the impact of global trade tensions on economic activity. The annual rate of GDP growth remained below-trend at 1.1%.

Then coronavirus swiftly changed everything. COVID-19, which had first appeared in China in December 2019, started spreading across the globe causing plummeting sentiment and falls in financial markets not seen since the Global Financial Crisis as part of a flight to quality into sovereign debt and other perceived 'safe' assets.

In response to the spread of the virus and sharp increase in those infected, the government enforced lockdowns, central banks and governments around the world cut interest rates and introduced massive stimulus packages in an attempt to reduce some of the negative economic impact to domestic and global growth.

The Bank of England, which had held policy rates steady at 0.75% through most of 2019/20, moved in March to cut rates to 0.25% from 0.75% and then swiftly thereafter brought them down further to the record low of 0.1%. In conjunction with these cuts, the UK government introduced a number of measures to help businesses and households impacted by a series of ever-tightening social restrictions, culminating in pretty much the entire lockdown of the UK.

The US economy grew at an annualised rate of 2.1% in Q4 2019. After escalating trade wars and a protracted standoff, the signing of Phase 1 of the trade agreement between the US and China in January was initially positive for both economies, but COVID-19 severely impacted sentiment and production in both countries. Against a slowing economic outlook, the US Federal Reserve began cutting rates in August. Following a series of five cuts, the largest of which were in March 2020, the Fed Funds rate fell from of 2.5% to range of 0% - 0.25%. The US government also unleashed a raft of COVID-19

related measures and support for its economy including a \$2 trillion fiscal stimulus package. With interest rates already on (or below) the floor, the European Central Bank held its base rate at 0% and deposit rate at -0.5%.

Financial markets: Financial markets sold off sharply as the impact from the coronavirus worsened. After starting positively in 2020, the FTSE 100 fell over 30% at its worst point with stock markets in other countries seeing similar huge falls. In March sterling touch its lowest level against the dollar since 1985. The measures implemented by central banks and governments helped restore some confidence and financial markets have rebounded in recent weeks but remain extremely volatile. The flight to quality caused gilts yields to fall substantially. The 5-year benchmark falling from 0.75% in April 2019 to 0.26% on 31st March. The 10-year benchmark yield fell from 1% to 0.4%, the 20-year benchmark yield from 1.47% to 0.76% over the same period. 1-month, 3-month and 12-month bid rates averaged 0.61%, 0.72% and 0.88% respectively over the period.

Since the start of the calendar 2020, the yield on 2-year US treasuries had fallen from 1.573% to 0.20% and from 1.877% to 0.61% for 10-year treasuries. German bund yields remain negative.

Credit review: In Q4 2019 Fitch affirmed the UK's AA sovereign rating, removed it from Rating Watch Negative (RWN) and assigned a negative outlook. Fitch then affirmed UK banks' long-term ratings, removed the RWN and assigned a stable outlook. Standard & Poor's also affirmed the UK sovereign AA rating and revised the outlook to stable from negative. The Bank of England announced its latest stress tests results for the main seven UK banking groups. All seven passed on both a common equity Tier 1 (CET1) ratio and a leverage ratio basis. Under the test scenario the banks' aggregate level of CET1 capital would remain twice their level before the 2008 financial crisis.

After remaining flat in January and February and between a range of 30-55bps, Credit Default Swap spreads rose sharply in March as the potential impact of the coronavirus on bank balance sheets gave cause for concern. Spreads declined in late March and through to mid-April but remain above their initial 2020 levels. NatWest Markets Plc (non-ringfenced) remains the highest at 128bps and National Westminster Bank Plc (ringfenced) still the lowest at 56bps. The other main UK banks are between 65bps and 123bps, with the latter being the thinly traded and volatile Santander UK CDS.

While the UK and Non-UK banks on the Arlingclose counterparty list remain in a strong and well-capitalised position, the duration advice on all these banks was cut to 35 days in mid-March.

Fitch downgraded the UK sovereign rating to AA- in March which was followed by a number of actions on UK and Non-UK banks. This included revising the outlook on all banks on the counterparty list to negative, with the exception of Barclays Bank, Rabobank, Handelsbanken and Nordea Bank which were placed on Rating Watch Negative, as well as cutting Close Brothers long-term rating to A-. Having revised their outlooks to negative, Fitch upgraded the long-term ratings on Canadian and German banks but downgraded the long-term ratings for Australian banks. HSBC Bank and HSBC UK Bank, however, had their long-term ratings increased by Fitch to AA-.

Counterparty	Length	From	To	Amount	Rate
Goldman Sachs MMF	Overnight	31/03/2020	01/04/2020	2,000,000.00	0.48%
Blackrock MMF	Overnight	31/03/2020	01/04/2020	1,700,000.00	0.49%
Aberdeen Asset Management MMF	Overnight	31/03/2020	01/04/2020	1,000,000.00	0.61%
Federated Investors MMF	Overnight	31/03/2020	01/04/2020	3,000,000.00	0.57%
CCLA MMF	Overnight	31/03/2020	01/04/2020	1,000,000.00	0.59%
Lloyds Main	Overnight	31/03/2020	01/04/2020	745,274.47	0.00%
Bank of Scotland	Overnight	31/03/2020	01/04/2020	1,795,000.01	0.00%
Santander Notice Account	95 days	31/03/2020	18/06/2020	1,495,000.00	0.85%
Northumberland County Council	1096	03/04/2017	03/04/2020	3,000,000.00	0.99%
Thurrock Council	365	02/04/2019	01/04/2020	1,000,000.00	1.00%
London Borough of Brent	274	18/11/2019	18/08/2020	5,000,000.00	0.90%
North Lanarkshire Council	275	02/12/2019	02/09/2020	5,000,000.00	0.87%
Lloyds Bank Fixed Term Deposit	182	20/11/2019	20/05/2020	1,500,000.00	0.80%
Eastleigh Borough Council	122	16/12/2019	16/04/2020	3,000,000.00	0.73%
Blackburn with Darwen Council	182	10/02/2020	10/08/2020	3,000,000.00	0.85%
Blackpool Borough Council	182	29/01/2020	29/07/2020	5,000,000.00	0.90%
Islington Council	182	20/01/2020	20/07/2020	3,000,000.00	0.85%
Ards and North Down Borough Council	261	13/01/2020	30/09/2020	2,000,000.00	0.95%
Kingston-upon-Hull City Council	185	13/03/2020	14/09/2020	2,000,000.00	0.90%
Broxtowe Borough Council	182	30/01/2020	30/07/2020	2,000,000.00	0.85%
Telford & Wrekin Council	184	09/03/2020	09/09/2020	2,500,000.00	1.17%
Total				50,735,274.48	

Policies and other considerations, as appropriate	
Council Priorities:	Value for Money
Policy Considerations:	Treasury Management Strategy Statement
Safeguarding:	Not Applicable
Equalities/Diversity:	Not Applicable
Customer Impact:	Not Applicable
Economic and Social Impact:	Not Applicable
Environment and Climate Change:	Not Applicable
Consultation/Community Engagement:	Not Applicable
Risks:	Borrowing and investment both carry an element of risk. This risk is mitigated through the adoption of the Treasury and Investment Strategies, compliance with the CIPFA code of Treasury Management and the retention of Treasury Management Advisors (Arlingclose) to proffer expert advice
Officer Contact	Anna Wright Finance Team Manager & Deputy S151 Officer anna.wright@nwleicestershire.gov.uk

This page is intentionally left blank

NORTH WEST LEICESTERSHIRE DISTRICT COUNCIL

AUDIT AND GOVERNANCE COMMITTEE – WEDNESDAY,
22 JULY 2020



Title of Report	PROGRESS OF IMPROVEMENTS IDENTIFIED THROUGH ANNUAL GOVERNANCE REVIEW 2018/19	
Presented by	Tracy Bingham Head of Finance and Section 151 Officer	
Background Papers	None	Public Report: Yes
Purpose of Report	To provide Committee members with an update in respect of progress made against improvements identified as part of the 2018/19 Annual Governance Statement.	
Recommendations	THAT THE AUDIT AND GOVERNANCE COMMITTEE NOTES AND COMMENTS ON THE REPORT	

1.0 BACKGROUND

- 1.1 Members reviewed and approved the Annual Governance Statement (AGS) in respect of the 2018/19 year at its meeting on 24 July 2019.
- 1.2 A total of 9 improvement areas identified through this review, where it was recognised that the Council could strengthen its governance arrangements. There are five improvements carried forward from the previous year's (2017/18) AGS and a further four identified during 2018/19. These improvements were scored as fair, meaning that satisfactory governance exists in these areas but improvements are required to meet good governance. There were no significant issues identified for 2018/19.
- 1.3 Committee members have agreed that progress against improvement areas will be reported at regular intervals and the AGS of future years will report on the progress/completion of improvements areas or significant issues from the prior period.
- 1.4 This update is the second update members have received on the progress of 2018/19 improvements.

2.0 PROGRESS MADE IN RESPECT OF IMPROVEMENT AREAS 2018/19

- 2.1 Of the 9 improvements identified, 4 are complete and the remaining 5 are underway.
- 2.2 Full details can be found in Appendix A.

Policies and other considerations, as appropriate	
Council Priorities:	Good governance underpins the council's ability to deliver against all of its priorities.
Policy Considerations:	None.
Safeguarding:	None.
Equalities/Diversity:	None.
Customer Impact:	None.
Economic and Social Impact:	None.
Environment and Climate Change:	None.
Consultation/Community Engagement:	None.
Risks:	None.
Officer Contact	Tracy Bingham Head of Finance and Section 151 Officer tracy.bingham@nwleicestershire.gov.uk

**PROGRESS MADE IN RESPECT OF IMPROVEMENTS IDENTIFIED THROUGH THE REVIEW OF
THE ANNUAL GOVERNANCE STATEMENT 2018/19**

Improvement	CIPFA / SOLACE Principle	Owner	Update 4 December 2019	Update 17 March 2020
Develop guidance on our approach to consultation as part of the communications strategy (carried forward from 2017/18 Annual Governance Statement Review).	Principle B	Head of Legal and Commercial Services	Underway. We will be providing guidance on the legal requirements on consultation – this will be rolled out in January 2020.	Complete. Guidance rolled out to Directors, heads of Service and Team Managers in February 2020.
Review approach to presenting the economic, social and environmental impact of decisions within committee reports.	Principle C	Head of Legal and Commercial Services	Complete. Revised committee report format adopted November 2019.	Complete.
Develop organisational requirements for benchmarking of services.	Principle E	Head of HR and Organisational Development	Underway. We will be collating information about benchmarking possibilities from the Team planning process in late 2019 / early 2020 to identify our future organisational approach.	Underway. Future organisational approach remains under development.
Corporate Asset Management Strategy required to go with HRA Asset Management Strategy (carried forward from 2017/18 Annual Governance Statement Review).	Principle E	Head of Housing and Property	Complete. The Corporate Asset Management Strategy was considered by Corporate Scrutiny Committee on 4 September 2019 and will be approved by Cabinet on 12 November 2019.	Complete.
Implement internal audit recommendations in respect of Health and Safety arrangements. Progress against this action will be reported via the Internal Auditors updates at Audit and Governance Committee.	Principle F	Head of HR and Organisational Development	Underway. Good progress being made with the support of an external critical friend from another Council, and we are procuring a new Health and Safety Management system/process. A joint management / trade union group has been established to consider and	Underway. New system (SHE) has been procured and implementation is underway. Health and Safety Task Group continues to meet to progress the other audit recommendations.

			progress the Health and Safety Audit report recommendations	
Review implementation of In-Phase and scope improvements to performance and project management frameworks. Develop performance management framework.	Principle F	Head of HR and Organisational Development	Complete. Changes to InPhase performance management and team planning arrangements including training completed for 2020/21. Quarterly reports to members have been changed and improved to focus on Council delivery plan delivery and key performance indicators. Project support arrangements are being changed to provide a level of administrative support. A corporate Performance management process has been completed.	Complete.
Completion of anti-fraud actions identified as part of anti-fraud and corruption audit to be completed (carried forward from 2017/18 Annual Governance Statement Review). Awareness raising of anti- fraud and corruption to take place amongst staff. Implement recommendations arising from the LCC review.	Principle F	Head of Finance	Underway. The Leicestershire Fraud Hub were commissioned early 2019 to undertake a review of the Council's fraud policy framework. The assessment and result of this work are yet to be received, following which, a programme of awareness raising will be developed and implemented.	Underway. Assessment completed by Leicester City Council and Action Plan now developed to implement recommendations including undertaking policy reviews, issuing revised policy to all staff and undertake awareness raising activity.
Implement actions identified within the Finance and Business Plan including the procurement of a new finance system (carried forward from 2017/18 Annual Governance Statement Review).	Principle F	Head of Finance	Underway. A range of improvement actions included in the plan have been implemented or started during the year so far including: - Work has commenced to procure a new finance system, with consultants appointed to develop a specification to go to the market. The timetable for procurement remains in development but	Underway. Further progress has been made with regards to the development of a specification for procuring a new finance system. The target date for issuing the invitation to tenders is Q1 2020/21. Going forward, actions arising from the Finance and Business Plan that are not related to the procurement of a new

			<p>we anticipate to have awarded a new finance system contract by July 2020.</p> <ul style="list-style-type: none"> - An new standardised investment appraisal approach has been developed and adopted by CLT - Pricing strategies for each income generating service areas are under development - The approach to scenario modelling in the council's medium term financial plan has been further developed - Training has been undertaken for the Extended Leadership Team in respect of budgeting. CLT have attended Treasury Management training. 	<p>finance system will be taken forward as part of the Journey to Self-Sufficiency Programme.</p>
<p>Implement actions to address issues identified in Internal Audit of Sundry Debtors (carried forward from 2017/18 Annual Governance Statement Review).</p>	<p>Principle F</p>	<p>Head of Finance</p>	<p>Underway. All recommendations arising from the sundry debtor internal audit have now been implemented with the exception of an action plan for dealing with historic sundry debts which is currently being reviewed by the Finance Team Manager. Internal Audit are in the process of finalising their follow-up review.</p>	<p>Complete. Action plan for dealing with historic debts developed and now in play and therefore all recommendations from the internal audit have now been implemented. Work to deal with historic debts continues and additional resource has been deployed to complete this.</p>

This page is intentionally left blank

NORTH WEST LEICESTERSHIRE DISTRICT COUNCIL

AUDIT AND GOVERNANCE COMMITTEE – WEDNESDAY,
22 JULY 2020

Title of Report	REVIEW OF CORPORATE GOVERNANCE POLICIES	
Presented by	Tracy Bingham Head of Finance	
Background Papers	UK Anti-corruption strategy 2017-2022 Bribery Act 2010 Data Protection Act 2018 Money Laundering and Terrorist Financing (Amendment) Regulations 2019 Investigatory Powers Act 2016 Home Office Codes of Practice 2018	Public Report: Yes
Purpose of Report	To receive the committee's comments on the Councils Governance Policies ahead of Cabinet	
Recommendations	THAT THE COMMITTEE PROVIDES ANY COMMENTS IT MAY HAVE FOR CONSIDERATION BY CABINET WHEN IT MEETS TO CONSIDER THE POLICIES ON 22 SEPTEMBER 2020.	

1.0 BACKGROUND

- 1.1 The Council is responsible for ensuring that its business is conducted in accordance with the law and appropriate standards. In discharging this responsibility the Council has in place arrangements for governance of its affairs and staff.
- 1.2 The following documents constitute the Council's suite of Corporate policies:

Policy	Last reviewed
Anti-Fraud and Corruption Policy;	2015
Anti-Money Laundering Policy;	2015
RIPA Policy	2016
Information Management	Not been to members
Data Protection Policy	Not been to members
Confidential Reporting (Whistleblowing) Policy;	2016
ICT & Cyber Security Policy;	2019

Risk Management Strategy;	2018
Local Code of Corporate Governance	2017

- 1.4 A comprehensive 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 22 September 2020.

2.0 POLICY REVIEWS

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

The main changes to each policy are summarised below:

2.1 Anti-Fraud and Corruption Policy

An internal audit in 2016/2017 recommended that a review of the Council's fraud policy framework be undertaken to confirm the Council's Policies were up to date. In 2018 Leicester City Council undertook the review on behalf of the District Council concluding that the Anti-Fraud and Corruption and Anti-Money Laundering policies should be updated.

The following changes to the Anti-Fraud and Corruption Policy have been made:

- A clarification of the definitions of Corruption and Bribery to reflect those in the HM Government – UK Anti-corruption strategy 2017-22 and the Bribery Act 2010.
- The reinforcement of the culture of the Council's opposition to Fraud and Corruption
- Setting out the commitment to take action against those who offend against the Council
- Setting out the commitment to take disciplinary action where there is a breach of the policy
- An update to the details of external auditors, to reflect the new 5 year contract
- A clarification of the role and responsibility of CLT
- Outlining how the policy complies with new Data Protection legislation, the Data Protection Act 2018

2.2 Anti-Money Laundering Policy

The following changes to the Anti-money Laundering Policy have been made:

- An update to the Councils commitment to reflect the new legislation, Money Laundering and Terrorist Financing (Amendment) Regulations 2019
- An update to the definition of Money Laundering to give a more detailed definition within the policy
- An update to the details of the Money Laundering Reporting Officer (MLRO) and deputy MLRO as new appointments have been made since the last policy

2.3 Confidential Reporting (Whistleblowing Policy)

The following changes to the Confidential Reporting (Whistleblowing) Policy have been made:

- A clarification of the application of legislation to reflect the changes that it has to be in the public interest and only covers workers.
- The refinement of the Policy aims to be specific as to who the policy covers
- An update to the contact details of the officer to whom concerns should be raised due to structural changes
- An update to reference the new Data Protection legislation, the Data Protection Act 2018

2.4 Risk Management Policy

The following changes to the Risk Management Policy have been made:

- The adoption of a regular review of the Risk Management Strategy every two years.
- A move to a more specific, mitigation based and regular review approach.
- Audit and Governance Committee to receive regular updates of the Risk Register and mitigation plans.
- A clarification on some reporting issues in terms of when and what groups and meetings are involved.
- The provision of additional clarity regarding the role of particular staff roles and responsibilities.
- An update to reflect current practice in terms of timing and process.
- Editorial 'tidying up' and updating.
- A commitment to continue to review the corporate risks quarterly and recommend any changes through CLT prior to the information being presented to this Committee and onwards to Cabinet.

2.5 RIPA Policy

In June 2020 a virtual inspection by the Investigatory Powers Commissioner's Office was undertaken and further to this the following changes have been made to the Corporate Policy and Procedure on the Regulation of Investigatory Powers Act 2000 (RIPA) Policy:

- An amendment of the policy name to include reference to new legislation, the Investigatory Powers Act 2016 (IPA);
- The addition of reference to the IPA, what it authorises and how to obtain an authorisation. The IPA governs the acquisition of communications data, for example the address to which a letter is sent, the time and duration of a phone call, the telephone number or e-mail address of the originator and recipient, and the location of the device from which a communication was made;
- The addition of reference to the most up to date codes of practice from the Home Office;
- The addition of reference to changes in how children (under 18s) can be used as informants (known as Covert Human Intelligence Sources);
- The addition of reference to the use of the Council owned drone:
 - Consideration should be given to whether or not the drone will capture personal information;

- If personal information is likely to be captured:
 - persons should be notified in advance (so it does not constitute covert surveillance); and
 - consider how to minimise this intrusion into people's privacy;
- The inclusion of a warning to staff not to use personal devices (e.g. mobile phones or computers) to carry out investigations for work purposes (e.g. accessing a person of interest's social media account from a personal device);
- An update to include reference to data retention periods to ensure any information obtained is deleted in accordance with the Council's Information Management Policy.

2.6 Information Management Policy

The following changes to the Information Management Policy have been made:

- A style change – update of the logo used
- An update to Information Management Team Structure and reference to corporate Information Champions
- The inclusion of reference to the Privacy and Electronic Communications Regulations (PECR) – This relates to the way data is used for marketing and is not limited to that which identifies personal data. Whilst the PCER have been in place since 2003, on the 25th May 2018 it became a requirement to comply with both PECR and GDPR. There is some overlap between the two but the overall aim is to protect data and complying with PECR helps comply with GDPR and vice versa.

As a result of the changes to working arrangements arising from COVID 19, the Council is working with other Leicestershire authorities to create a shared approach to dealing with homeworking within the policy. This will be brought forward at a later date.

2.7 Data Protection Policy

The Data Protection policy remains largely up to date as it was reviewed in 2019. The only amendments that have been made are to update the policy owner and reviewers.

These updates reflect the ownership of the policy and ensure that monitoring is objective.

2.8 ICT & Cyber Security Policy

The following changes to the ICT and Cyber Security Policy have been made:

- Spelling and grammar
- An update to some homeworking guidelines
- The inclusion of IT assets and how they are managed, as this was missing previously
- The addition of information relating to Cyber security including the process and procedure to report a cyber-incident
- An update to the use of 2 factor authentication and use of the Swivel mobile App
- The addition of I information about virtual meetings and the privacy of those meetings

2.9 Local Code of Corporate Governance

The Local Code of Corporate Governance continues to reflect the Council's current corporate governance arrangements and therefore only presentational and contextual changes have been made.

The Code was last reviewed and updated in 2017 in line with joint guidance on corporate governance by the Chartered Institute of Public Finance & Accountancy (CIPFA) and the Society of Local Authority Chief Executives (SOLACE)

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

This page is intentionally left blank

ANTI-FRAUD AND CORRUPTION POLICY

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

Version Control

Version No.	Author	Date
2.1	Anna Wright, Senior Auditor	September 2015
2.2	Lisa Marron, Audit Manager	October 2019
2.3	Kerry Beavis, Senior Auditor	May 2020

**Version 2.3
May 2020**

	Contents	Page No.
1.	Introduction	3
2.	Scope	3
3.	Definitions	3
4.	Culture	4
5.	Responsibilities	5
6.	Prevention and Deterrence	7
7.	Detection and Investigation	9
8.	Raising Concerns	9

ANTI-FRAUD AND CORRUPTION POLICY

1. INTRODUCTION

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

2. SCOPE

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

3. DEFINITIONS

3.1 Fraud

- 3.1.1 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.

- 3.1.2 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.

- 3.1.3 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.

3.1.4 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

3.2.1 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

3.3.1 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

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

4. **CULTURE**

4.1 We have determined that the culture and tone of the organisation will be one of honesty and opposition to fraud and corruption. We will not tolerate malpractice or wrongdoing in the provision of our services and are prepared to take vigorous action to stamp out any instances of this kind of activity. The fight against fraud and corruption can only be truly effective where these acts are seen as anti-social unacceptable behaviour and whistle blowing is perceived as a public-spirited action.

4.2 The prevention/detection of fraud/corruption and the protection of public money are responsibilities of everyone, both internal and external to the organisation. The Council's elected members and employees play an important role in creating and maintaining this culture. They are positively encouraged to raise concerns regarding fraud and corruption, immaterial of seniority, rank or status, in the knowledge that such concerns will wherever possible be treated in confidence. The public also has a role to play in this process and should inform the Council if they feel that fraud/corruption may have occurred. The Nolan Committee on Standards in Public Life set out the seven guiding principles (Appendix A) that apply to people who serve the public.

4.3 Concerns must be raised when members, employees or the public reasonably believe that one or more of the following has occurred or is in the process of occurring or is likely to occur:

- a criminal offence;

- a failure to comply with a statutory or legal obligation;
- improper or unauthorised use of public or other official funds;
- a miscarriage of justice;
- maladministration, misconduct or malpractice;
- endangering an individual's health and/or safety;
- damage to the environment; and
- deliberate concealment of any of the above.

4.4 The Council will ensure that any allegations received in any way, including by anonymous letter or telephone call, will be taken seriously and investigated in an appropriate manner. The Council has a [Confidential Report \(Whistleblowing\) policy](#) that sets out the approach to these types of allegation in more detail.

4.5 The Council will take action against those who defraud the Council or who are corrupt or where there has been financial malpractice. There is, of course, a need to ensure that any investigation process is not misused and, therefore, any abuse (such as employees raising malicious allegations) may be dealt with as a disciplinary matter.

4.6 Where fraud or corruption has occurred due to a breakdown in the Council's systems or procedures, the Head of Service will ensure that appropriate improvements in systems of control are implemented in order to prevent re-occurrence.

5. RESPONSIBILITIES

5.1 Responsibilities of Elected Members

5.1.1 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

5.2.1 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

5.3.1 The Head of Finance 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'.

5.3.2 Under the Head of Finance's 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 anti-fraud and corruption framework of the Council.

5.4 Responsibilities of Employees

- 5.4.1 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.
- 5.4.2 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.
- 5.4.3 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

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

5.6 Role of the External Auditors

- 5.6.1 Independent external audit is an essential safeguard of the stewardship of public money. This is currently carried out by Mazars LLP 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

- 5.7.1 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

- 5.8.1 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

- 6.1.1 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.
- 6.1.2 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.
- 6.1.3 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

- 6.2.1 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

- 6.3.1 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)

- 6.4.1 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

- 6.5.1 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

- 6.6.1 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

- 6.7.1 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.
- 6.7.2 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

- 6.8.1 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

- 6.9.1 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.
- 6.9.2 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.
- 7.2 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.
- 7.3 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.
- 7.4 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.
- 7.5 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.
- 7.6 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: bev.smith@nwleicestershire.gov.uk
Telephone 01530 454500
- Monitoring Officer: elizabeth.warhurst@nwleicestershire.gov.uk
Telephone 01530 454762
- Section 151 Officer: tracy.bingham@nwleicestershire.gov.uk
Telephone 01530 454707
- Audit Manager: lisa.marron@nwleicestershire.gov.uk
Telephone 01530 454728

9. Review

- 9.1 This policy will be reviewed bi-annually or if legislation changes if this is sooner,

THE SEVEN PRINCIPLES OF PUBLIC LIFE

Selflessness

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

Integrity

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

Objectivity

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

Accountability

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

Openness

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

Honesty

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

Leadership

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

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

This page is intentionally left blank

ANTI-MONEY LAUNDERING POLICY

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

Version Control

Version No.	Author	Date
2.1	Anna Wright, Senior Manager	September 2015
2.2	Kerry Beavis, Senior Auditor	May 2020

**Version 2.2
May 2020**

	Contents	Page No.
1.	Introduction	3
2.	Scope of the Policy	3
3.	Definition of Money Laundering	3
4.	Requirements of the Money Laundering Legislation	4
5.	The Money Laundering Reporting Officer (MLRO)	4
6.	Client Identification Procedures	4
7.	Reporting Procedure and Suspensions of Money Laundering	5
8.	Consideration of the Disclosure by the MLRO	6
9.	Training	7
10.	Review	7

ANTI-MONEY LAUNDERING POLICY

1. INTRODUCTION

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

2. SCOPE OF THE POLICY

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

3. DEFINITION OF MONEY LAUNDERING

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

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

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

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

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

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

There are also two 'third party' offences:

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

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

- 3.2 The Terrorism Act made it an offence of money laundering to become concerned in an arrangement relating to the retention or control of property likely to be used for the purpose of terrorism, or resulting from acts of terrorism.
- 3.3 Although the term 'money laundering' is generally used to describe the activities of organised crime for most people it will involve a suspicion that someone they know, or know of, is benefiting financially from dishonest activities.
- 3.4 Potentially very heavy penalties (unlimited fines and imprisonment up to fourteen years) can be handed down to those who are convicted of one of the offences above.

4. REQUIREMENTS OF THE MONEY LAUNDERING LEGISLATION

- 4.1 The main requirements of the legislation are:
- to appoint a money laundering reporting officer;
 - maintain client identification procedures in certain circumstances;
 - implement a procedure to enable the reporting of suspicions of money laundering;
 - maintain record keeping procedures.

5. THE MONEY LAUNDERING REPORTING OFFICER (MLRO)

- 5.1 The Council has designated the Section 151 Officer as the Money Laundering Reporting Officer (MLRO). She can be contacted on 01530 454707 or at tracy.bingham@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. She can be contacted on 01530 454492 or at anna.wright@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 her to prepare her report to the National Crime Agency (NCA), where appropriate. You should also enclose copies of any relevant supporting documentation.

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

7.4 Once you have reported the matter to the MLRO you must follow any directions she may give you. You must NOT make any further enquiries into the matter yourself, any necessary investigation will be undertaken by the NCA. Simply report your suspicions to the MLRO who will refer the matter on to the NCA if appropriate. All members of staff will be required to co-operate with the MLRO and the authorities during any subsequent money laundering investigation.

7.5 Similarly, at no time and under no circumstances should you voice any suspicions to the person(s) whom you suspect of money laundering, even if the NCA has given consent to a particular transaction proceeding, without the specific consent of the MLRO; otherwise you may commit a criminal offence of 'tipping off'.

7.6 Do not, therefore, make any reference on a client file, to a report having been made to the MLRO - should the client exercise their right to see the file, then such a note will obviously tip them off to the report having been made and may render you liable to prosecution. The MLRO will keep the appropriate records in a confidential manner.

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

8.1 Upon receipt of a disclosure report, the MLRO must note the date of receipt on her section of the report and acknowledge receipt of it. She should also advise you of the timescale within which she expects to respond to you.

8.2 The MLRO will consider the report and any other available internal information she thinks 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 inquiries she thinks 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, she 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 she needs to seek consent from the NCA for a particular transaction to proceed.

8.4 Where the MLRO does so conclude, then she must disclose the matter as soon as practicable to the NCA on their standard report form and in the prescribed manner, unless she has 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 non-disclosure, then she must note the report accordingly, she can then immediately give her 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 she shall mark the report accordingly and give her consent for any ongoing or imminent transaction(s) to proceed.
- 8.8 All disclosure reports referred to the MLRO and reports made by her 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 she knows or suspects, or has reasonable grounds to do so, through a disclosure being made to her, that another person is engaged in money laundering and she does not disclose this as soon as practicable to the NCA.

9. TRAINING

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

10. REVIEW

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

This page is intentionally left blank

CONFIDENTIAL REPORTING (WHISTLEBLOWING) POLICY

Policy Statement

Version Control

Version No.	Author	Date
2.1	Kerry Beavis, Senior Auditor	May 2020

**Version 2.1
May 2020**

	Contents	Page No.
1.	Introduction	3
2.	Aims and Scope of this Policy	4
3.	Safeguards - Harassment or Victimisation	5
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

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 but not employed; and
 - self-employed workers, if supervised or working off-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 THIS POLICY

2.1 This Policy aims to:

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

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

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

3. SAFEGUARDS - HARASSMENT OR VICTIMISATION

3.1 The Council is committed to good practice and high standards and aims to be supportive of employees and others using this Policy.

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

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

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

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

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

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

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

4. CONFIDENTIALITY

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

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

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

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

5. ANONYMOUS ALLEGATIONS

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

6. UNTRUE ALLEGATIONS

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

7. HOW TO RAISE A CONCERN

- 7.1 Advice and guidance on how to pursue matters of concern may be obtained from the Council's nominated contact points who are:
- Chief Executive: bev.smith@nwleicestershire.gov.uk
Telephone 01530 454500
 - Monitoring Officer: elizabeth.warhurst@nwleicestershire.gov.uk
Telephone 01530 454762
 - Section 151 Officer: tracy.bingham@nwleicestershire.gov.uk
Telephone 01530 454707
 - Audit Manager: lisa.marron@nwleicestershire.gov.uk
Telephone 01530 454728
- 7.2 Concerns may be raised verbally or in writing, to any of the above named individuals. If raising a concern in writing, it should be addressed to the named individual at the:

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

Clearly mark the envelope “Confidential”.

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

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

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

8. HOW THE COUNCIL WILL RESPOND

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

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

- 8.4 In order to protect individuals and those accused of misdeeds or possible malpractice, the Council will undertake initial enquiries to decide whether an investigation is appropriate and, if so, what form it should take. In most cases, it is anticipated that these initial enquiries will be completed within ten working days of an allegation being made. The overriding principle which the Council will have in mind when deciding what steps to take is whether the matter falls within the public interest. Any concerns or allegations which fall within the scope of any other specific procedures (for example, misconduct or discrimination issues) will normally be referred to the relevant service area for consideration under those procedures.
- 8.5 Some concerns may be resolved by agreed action without the need for investigation. If urgent action is required this will be taken before any investigation is conducted.
- 8.6 Within seven working days of a concern being raised, the nominated contact will write to you:
- acknowledging that the concern has been received,
 - indicating how we propose to deal with the matter,
 - giving an estimate of how long it will take to provide a final response,
 - telling you whether any initial enquiries have been made,
 - supplying you with information on staff support mechanisms, and
 - telling you whether further investigations will take place and if not, why not.
- 8.7 The amount of contact between the officers considering the issues and you will depend on the nature of the matters raised, the potential difficulties involved and the clarity of the information provided. If necessary, the Council will seek further information from you.
- 8.8 Where any meeting is arranged, off-site if you so wish, you can be accompanied by a trade union or professional association representative or a friend.
- 8.9 The Council will take steps to minimise any difficulties which you may experience as a result of raising a concern. For instance, if you are required to give evidence in criminal or disciplinary proceedings the Council will arrange for you to receive advice about the procedure.
- 8.10 The Council accepts that you need to be assured that the matter has been properly addressed. Thus, subject to legal constraints, we will inform you of the outcome of any investigation.

9. THE RESPONSIBLE OFFICER

- 9.1 The Chief Executive has overall responsibility for the maintenance and operation of this Policy. That officer maintains a record of concerns raised and the outcomes (but in a form which does not endanger your confidentiality) and will immediately notify the Monitoring Officer and Section 151 Officer of all issues raised under this Policy and will report as necessary to the Council.

10. HOW THE MATTER CAN BE TAKEN FURTHER

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

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

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

11. Review

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

This page is intentionally left blank

RISK MANAGEMENT POLICY

Policy Statement

Version Control

Version No.	Author	Date
1		December 2014
2		May 2016
3	Andy Barton	May 2020

May 2020

	Contents	Page No.
1.	Introduction	3
2.	Risk Management Structure	3
3.	Aims of the Policy	3
4.	Risk Management Policy	4
5.	Corporate Risk Scrutiny Group	6
6.	Procedures	7
7.	Funding for Risk Management	7
8.	Benefits of Effective Risk Management	7

RISK MANAGEMENT POLICY

1. INTRODUCTION

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

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

2. RISK MANAGEMENT STRUCTURE

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

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

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

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

3. AIMS OF THE POLICY

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

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

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

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

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

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

4. RISK MANAGEMENT POLICY

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

(a) Identification / Consideration of Risks

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

- Externally horizon scan for impending risks that may impact the council, communicate the risk to the appropriate risk owner so they can assess for likelihood and impact, identify mitigating controls and allocate responsibility for 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 Risk Scrutiny Group is presented to Corporate Leadership Team for discussion and information on a quarterly basis.
- Develops arrangements to monitor and measure performance of risk management activities against the Council's strategic aims and priorities.
- Considers risks in relation to significant partnerships, which requires assurances to be obtained about the management of those risks.

(c) Member Involvement / Responsibility

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

(d) Training / Awareness

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

(e) Review

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

(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. CORPORATE RISK SCRUTINY GROUP

5.1 The Corporate Risk Scrutiny Group is made up of technical experts and corporate leads from the Council's Service Areas. Members of the Group act as "champions" for risk within their services and the Group provides a link into the CLT.

5.2 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.

6. PROCEDURES

- 6.1 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.

7. FUNDING FOR RISK MANAGEMENT

- 7.1 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.

8. BENEFITS OF EFFECTIVE RISK MANAGEMENT

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

Improved Strategic Management

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

Improved Operational Managements

- Reduction in interruptions to service delivery: fewer surprises!

- Reduction in managerial time spent dealing with the consequences of a risk event occurring
- Improved health and safety of employees and others affected by the Council's activities
- Compliance with legislation and regulations

Improved Financial Management

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

Improved Customer Service

- Minimal service disruption to customers and a positive external image

RISK MANAGEMENT FRAMEWORK

(A) What is the framework?

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

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

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

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

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

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

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

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

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

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

(C) Assessing risk

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

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

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

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

Table 1 - assessing the likelihood of exposure

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

Table 2 - assessing the impact of exposure

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

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

(D) Prioritisation of risk

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

Table 3 - a risk matrix

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

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

Table 4 - intended responses to risk

Red	Controls and/or mitigating actions are required to reduce the risk to an acceptable level. Effort should be focused on reducing the risk of any items appearing in this zone, hence moving them to the amber or green zone.
Amber	Risks will require ongoing monitoring to ensure they do not move into the red zone. Depending on the resources required to address

	the red risks, it may be appropriate to develop controls/mitigating actions to control these risks.
Green	Existing controls and/or mitigating actions are sufficient and may be excessive. More resource committed to reduce these risks is likely to be wasted. Consideration should be given to relaxing the level of control to release resources for mitigating higher level risks.

(E) **Format of the risk register**

Annex 1 to this framework provides a standard format.

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

This page is intentionally left blank

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

Version Control

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

June 2020

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

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

1. INTRODUCTION

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

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

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

2. TYPES OF SURVEILLANCE

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

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

3. CONDUCT AND USE OF COVERT HUMAN INTELLIGENCE SOURCES

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

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

Juvenile CHISs

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

4. OPEN SOURCE (ONLINE) COVERT ACTIVITY

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

5. USE OF PERSONAL DEVICES FOR BUSINESS USE

- 5.1 Using 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 used to gather **personal information** the subject of the surveillance will either need to be notified of the use of the drone (such that any surveillance is not **covert**) or a RIPA authorisation will be needed.
- 6.2 If the drone is to be used for publicity purposes, consideration must be given to the area the drone will be used and/or the event at which the drone will be used. The Council should avoid using the drone in residential areas as this is likely to capture **private information**. If this is not possible, residents should be notified in advance and consideration should be given to obtaining a RIPA authorisation. If the drone is to be used at public events, this should be made clear on any communications advertising the event.

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 Commercial 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 and the Directors are designated to act as Authorising Officers under the Constitution (Part 3, Sec 7, Para 3.3). The Chief Executive or Directors may designate other officers to act as Authorising Officers, provided these officers are of the level specified by the Secretary of State in the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 (i.e. Heads of Service can be designated as Authorising Officers).
- 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 Commercial 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 three 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, or the sending of a communication or breach of a person’s privacy.
- 9.8 A Local Authority may not make an application that requires the processing or disclosure of internet connection records for any purpose.

10. AUTHORISATION PROCESS - COMMUNICATIONS DATA

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

individual must complete a course of training appropriate for the role of a SPoC and have been issued the relevant SPoC unique identifier. The Home Office provides authentication services to enable telecommunications operators and postal operators to validate SPoC credentials;

- 10.1.3 The Senior Responsible Officer - Within every relevant public authority there should be a Senior Responsible Officer. The Senior Responsible Officer must be of a senior rank in a public authority. This must be at least the same rank as the designated senior officer specified in Schedule 4 of the IPA. Where no designated senior officer is specified the rank of the senior responsible officer must be agreed with the Home Office. In this Council the Senior Responsible Officer is the Chief Executive; 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 Commercial 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 authorises 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 Commercial 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 Commercial 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.

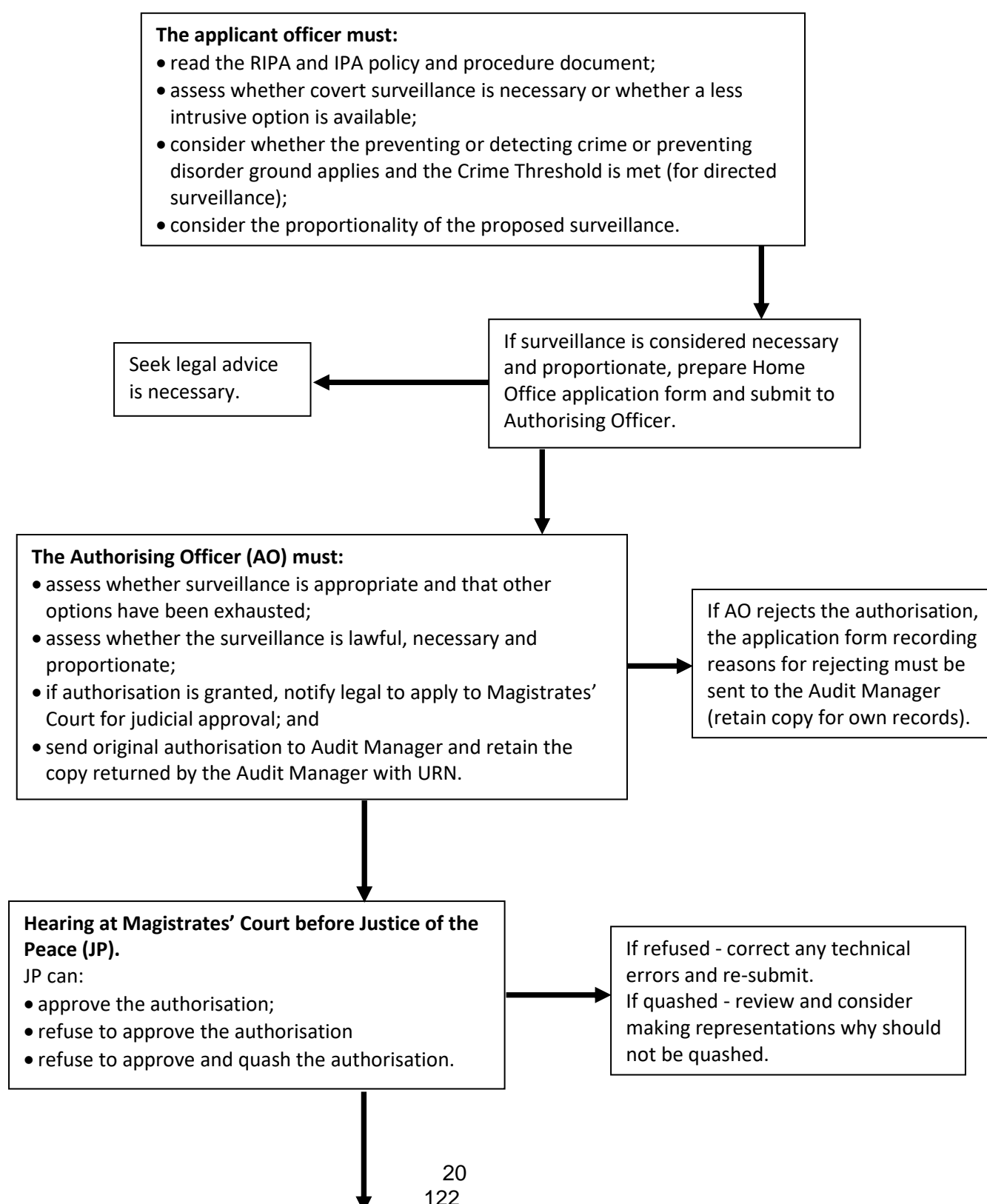
14.9 The Audit Manager co-ordinating RIPA and IPA applications ensures that there is an awareness of the investigations taking place. This would also serve to highlight any unauthorised **covert** surveillance being conducted.

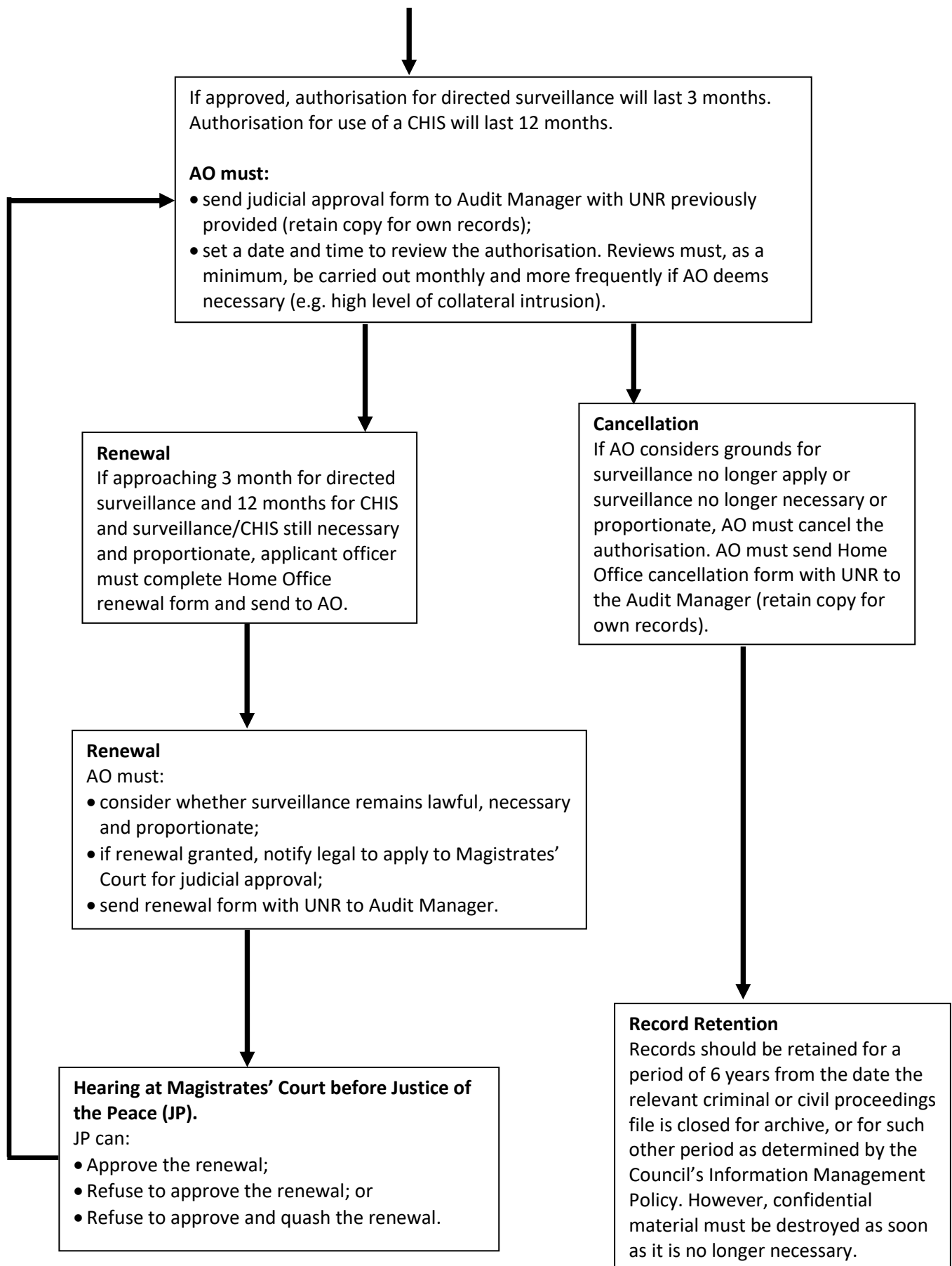
Retention and Destruction of Material

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 Commercial Services or the Senior Responsible Officer.

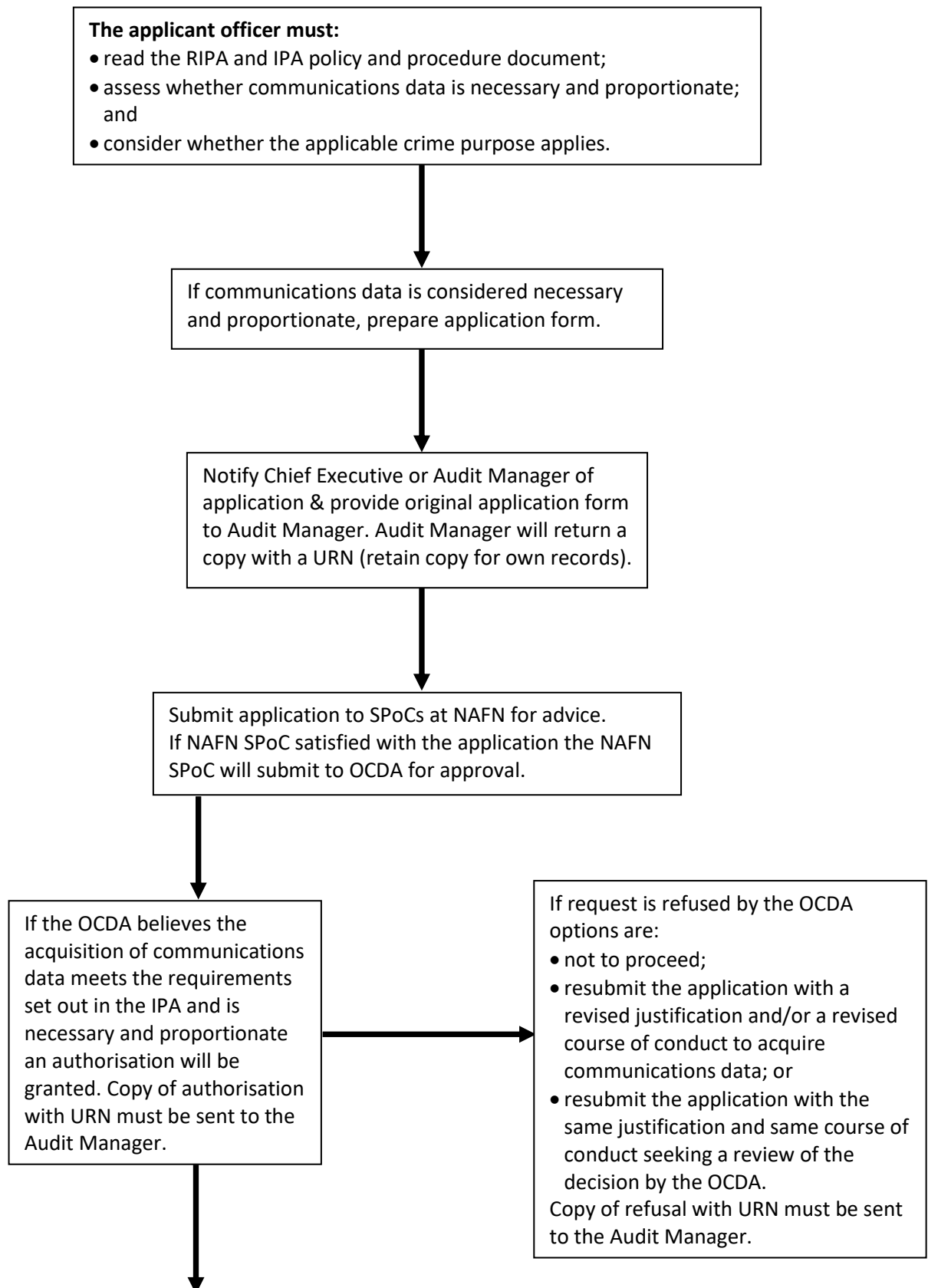
RIPA - AUTHORISATION OF DIRECTED SURVEILLANCE / USE OF A CHIS PROCEDURE

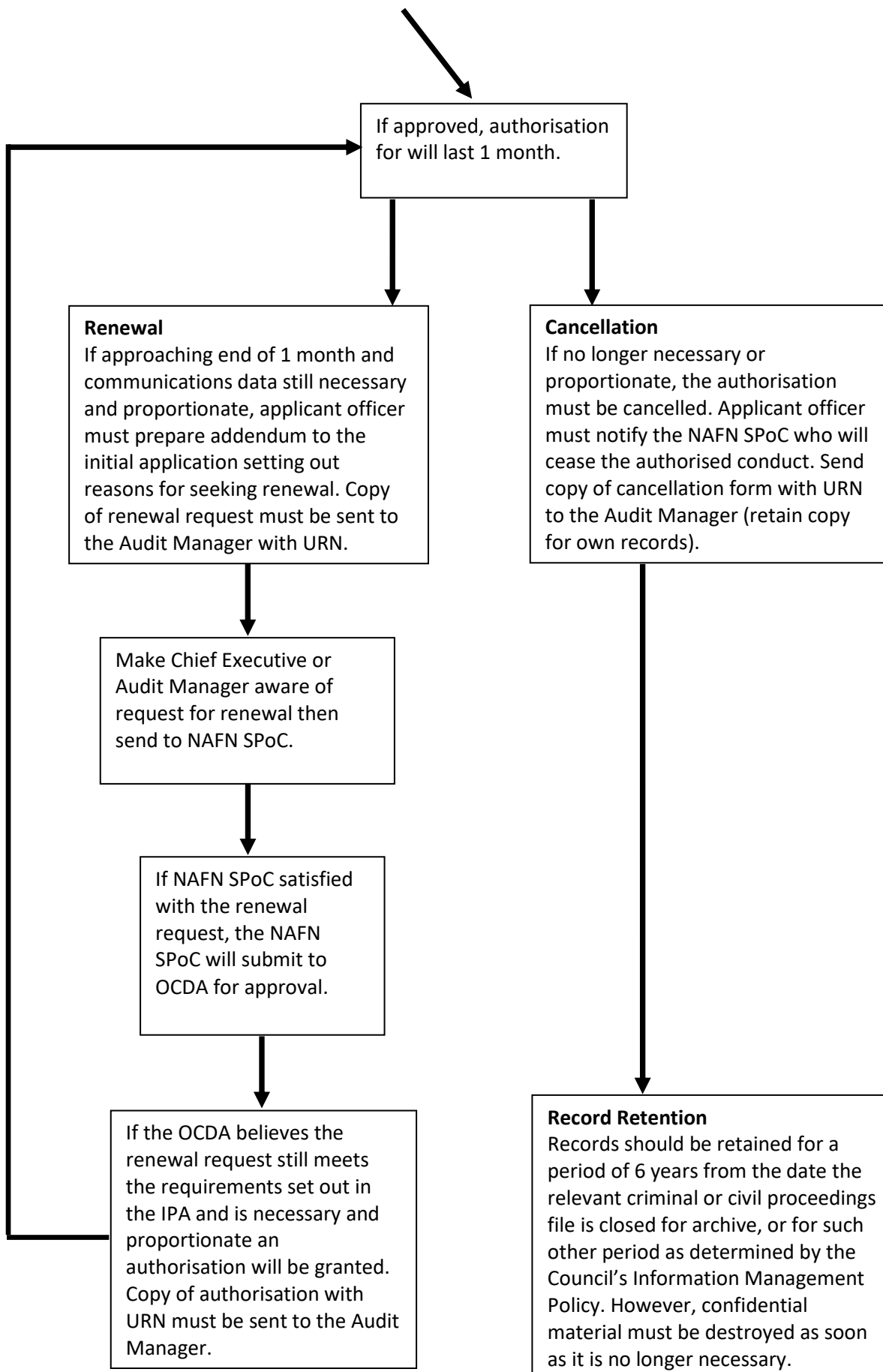
(Note: Note: Only the Chief Executive may authorise the use of a juvenile or vulnerable individual as a CHIS)





IPA - COMMUNICATIONS DATA AUTHORISATION PROCESS





This page is intentionally left blank

INFORMATION MANAGEMENT POLICY

Version Control

Version No.	Author	Date	Update Information
V1.0	Lynn Wyeth	20.11.2015	Original Draft
V1.1	Lynn Wyeth	04.12.2015	Amendments by NWLDC incorporated
V1.2	Lee Mansfield	15.12.2015	Amendment made following CLT decision - SIRO
V1.3	Lee Mansfield	02.02.2016	To reference legal as location of the IM team
V1.4	Sabrina Doherty	23.02.2017	Changes made to team structures, functions, roles and responsibilities
V1.5	Andrew Hickling / Louis Sebastian	09.05.2018	Changes made to team structures, functions, roles and responsibilities
V1.6	Nicola Taylor / Mackenzie Keatley	01.07.2020	Change made to team structures, roles and responsibilities, training and support, legislation update

June 2020

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

INFORMATION MANAGEMENT POLICY

POLICY STATEMENT

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

1. INTRODUCTION

1.1 The key areas of Information Management are:

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

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

2. PURPOSE OF THE POLICY

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

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

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

3. SCOPE OF THIS POLICY

3.1 This policy, framework and supporting policies apply to:

- all information systems within the organisation (both electronic and paper based);
- all data, information, and records owned by the Council, but also including those held by contractors or partner organisations on behalf of, or as a result of their relationship with, the Council);

- any information that is owned by other organisations, but may be accessed and used by Council employees;
 - information in whatever storage format and however transmitted (i.e., paper, voice, photo, video, audio or any digital format. It will also cover formats that are developed and used in the future.);
 - all employees of the Council, Council members, temporary workers, volunteers, student placements, etc;
 - the employees of any other organisations having access to Council information, for example, auditors, contractors, and other partner agencies where there is no specific information sharing protocol in place,
- 3.2 The procedures outlined in this Policy are in addition to the Council's complaints procedures and other statutory reporting procedures applying to some divisions.
- 3.3 This Policy has been discussed with the relevant trade unions and has their support.

4. PROCEDURES AND GUIDANCE

- 4.1 This Information Management Policy will be strengthened by other associated Council policies / procedures / material including but not limited to:
- ICT Security Policy;
 - Request for Information Procedure;
 - Security Incident Procedure;
 - Records Management Procedure;
 - Information Sharing Procedure;
 - Whistleblowing Policy;
 - RIPA Policy;
 - Anti-Money Laundering Policy;
 - Employment Practices Code - Information Commissioner's Office.

5. PRINCIPLES OF INFORMATION MANAGEMENT

- 5.1 The Council understands the need for an appropriate balance between openness and confidentiality in the management and use of information. The Council also understands the need to share information with others in a controlled manner.
- 5.2 To maximise the value of organisational assets the Council will endeavour to ensure that data is:
- held securely and confidentially;
 - obtained fairly and lawfully;
 - recorded accurately and reliably;
 - used effectively and ethically;
 - shared and disclosed appropriately and lawfully;
- 5.3 To protect the organisation's information assets from all threats, whether internal or external, deliberate or accidental, the Council will ensure:
- information will be protected against unauthorised access;
 - confidentiality of information will be assured;
 - integrity of information will be maintained;
 - information will be supported by the highest quality data;

- regulatory and legislative requirements will be met;
- business continuity plans will be produced, maintained and tested;
- information security training will be mandatory for all staff;
- all breaches of information security, actual or suspected, will be reported via the Security Incident Procedure and investigated by the Data Protection Officer or Information Management Officer;
- significant breaches will be handled with support from Human Resources and/or ICT Manager and/or Legal Services;

6. ROLES AND RESPONSIBILITIES

6.1 Information Asset Owners

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

6.1.2 Information Asset Owners will:

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

6.2 Senior Information Risk Owner

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

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

6.3 Data Protection Officer

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

Under GDPR it is mandatory that a public authority appoint a Data Protection Officer (DPO).

The DPO's tasks are defined in Article 39 of the GDPR.

The DPO Information Management responsibilities include:

- implementing information management procedures and processes for the organisation;
- raising awareness about information management to all staff;
- ensuring that training is provided annually and is completed by all staff;

- co-ordinating the activities of any other staff given responsibilities for data protection, confidentiality, information quality, records management and Freedom of Information;
- conducting internal audits to ensure compliance on an ad-hoc basis;
- ensures the Council is responsible for the continued integrity of datasets and maintains and enforces applications of policies and standards;
- to co-operate with the supervisory authority (ICO).

6.4 Information Governance

6.4.1 Information management is co-ordinated and managed by the Information Governance Team. The Team will:

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

6.5 ICT Team Manager

6.5.1 The ICT Team Manager is responsible for:

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

6.6 Head of Service / Team Managers

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

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

- where to get advice on security issues and how to report suspected security incidents.

6.7 Staff

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

- policy / strategy and procedure manuals;
- their line manager;
- the legal team;
- specific training courses;
- other communication methods, for example, team meetings; and staff intranet.

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

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

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

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

7. **MAIN THEMES**

7.1 Openness

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

7.2 Legal Compliance

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

7.3 Information Security

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

7.4 Information and Records Management

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

7.5 Information Quality Assurance

- 7.5.1 The Council will undertake or commission regular assessments and audits of its information quality and records management arrangements.
- 7.5.2 Managers are expected to take ownership of, and seek to improve, the quality of data within their services. Training and awareness-raising sessions appropriate to staff groups will be provided.

7.6 Partnerships and Information Sharing

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

8. RISK

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

9. TRAINING

- 9.1 Appropriate training will be mandatory for all staff.
- 9.2 All staff will be made aware of their obligations for information management through effective communication programmes.
- 9.3 Each new employee will be made aware of their obligations for information management during an induction-training programme and will be required to undergo mandatory data protection training before they can pass their probation period.
- 9.4 Training requirements will be reviewed annually to ensure that staff are adequately trained.

10. COMPLIANCE

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

11. FEES AND CHARGES

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

12. COMPLAINTS

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

- DPO@NWLeicestershire.gov.uk (personal data requests)
- FOI@NWLeicestershire.gov.uk (non-personal information request)
- Data Protection Officer
North West Leicestershire District Council
Whitwick Road
Coalville
Leicestershire
LE67 3FJ

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

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

13. EQUALITIES IMPACT ASSESSMENT

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

14. REVIEW OF POLICY

- 14.1 This policy will be reviewed as deemed appropriate, especially in light of any legislative changes, but no less frequently than every 12 months.

14.2 Policy review will be undertaken by the Information Governance Team.

DATA PROTECTION POLICY

Version Awareness

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

Version Control

Version No.	Author	Date Issued	Update Information
V1.0	B Wilson	21.05.2018	Original approved version.
V1.1	N Taylor	28.01.2019	Amended to reflect updated policy.
V1.2	N Taylor	28.05.2020	Updated Sections 4.2, 8.1 and 9.1

May 2020

	Contents	Page No.
1.	Introduction	3
2.	What Information is Covered?	4
3.	Policy Statement	4
4.	Principles	4
5.	Scope of this Policy	5
6.	Policy	5
7.	Data Protection Responsibilities	5
8.	Monitoring	6
9.	Validity of this Policy	7
	Appendices	
	Appendix A - GDPR 2018 - Data Protection Principles	8
	Appendix B - Summary of Relevant Legislation and Guidance	9
	Appendix C - Rights of Data Subjects	11

DATA PROTECTION POLICY

1. INTRODUCTION

Background

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

Data Protection and the GDPR Principles

- 1.7 NWLDC has a legal obligation to comply with all relevant legislation in respect of data protection and information / IT security. The organisation also has a duty to comply with guidance issued by the Information Commissioners Office.
- 1.8 All legislation relevant to an individual's right to the confidentiality of their information and the ways in which that can be achieved and maintained are paramount to the Council. Significant penalties can be imposed upon the organisation or its employees for non-compliance.
- 1.9 The aim of this policy is to outline how the NWLDC meets its legal obligations in safeguarding confidentiality and adheres to information security standards. The obligations within this policy are principally based upon the requirements of the DPA and GDPR, as the key legislative and regulatory provisions governing the security of person-identifiable information.

- 1.10 Other relevant legislation and guidance referenced and to be read in conjunction with this policy, is outlined together with a brief summary at Appendix B (below).
- 1.11 GDPR requires Public Authorities to appoint a Data Protection Officer. A Data Protection Officer (DPO) is an enterprise security leadership role required by the General Data Protection Regulation (GDPR). Data Protection Officers are responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements.

2. WHAT INFORMATION IS COVERED

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

3. POLICY STATEMENT

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

It sets out:

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

4. PRINCIPLES

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

- **To ensure notification;**

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

- **To ensure professionalism;**

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

- **To preserve security;**

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

- **To ensure awareness;**

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

- **Data Subject Access;**

Prompt and informed responses to subject access requests.

- 4.2 The policy will be reviewed periodically by the NWLDC Information Governance Team. Where review and update is necessary due to legislative changes this will be done immediately.
- 4.3 In accordance with the council's equality and diversity policy statement, this procedure will not discriminate, either directly or indirectly, on the grounds of gender, race, colour, ethnic or national origin, sexual orientation, marital status, religion or belief, age, union membership, disability, offending background or any other personal characteristic.

5. SCOPE OF THIS POLICY

- 5.1 This policy will ensure that person-identifiable information is processed, handled, transferred, disclosed and disposed of lawfully. Person-identifiable information should be handled in the most secure manner by authorised staff only, on a need to know basis.
- 5.2 The procedures cover all person identifiable information, electronic or paper which may relate to employees, contractors and third parties about whom we hold information.

6. POLICY

- 6.1 NWLDC obtains and processes person-identifiable information for a variety of different purposes, including but not limited to:
 - staff records and administrative records;
 - Service Users records including the administering of benefits, council tax, housing records, elections, grants, planning applications, licensing applications, etc;
 - matters relating to the prevention, detection and investigation of offences, fraud and corruption;
 - matters relating to the enforcement of primary and secondary legislation;
 - complaints and requests for information.
- 6.2 Such information may be kept in either computer or manual records. In processing such personal data, NWLDC will comply with the data protection principles within the DPA and GDPR.

7. DATA PROTECTION RESPONSIBILITIES

Overall Responsibilities

- 7.1 The Council is the 'data controller' and permits the organisation's staff to use computers and relevant filing systems (manual records) in connection with their duties. The Council has legal responsibility for the notification process and compliance with the DPA and the GDPR.
- 7.2 The Council whilst retaining its legal responsibilities has delegated data protection compliance to the Data Protection Officer.

Data Protection Officer's (DPO) Responsibilities

7.3 The Data Protection Officer's responsibilities include:

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

Line Managers' Responsibilities

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

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

General Responsibilities

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

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

7.7 All NWLDC employees will, on receipt of a request from an individual for information held, known as a subject access request or concerns about the processing of personal information, immediately notify the Compliance Officer.

7.8 Employees must follow the subject access request procedure (see Appendix C below).

8. MONITORING

8.1 Compliance with this policy will be monitored by the Corporate Leadership Team, together with internal audit reviews where necessary.

8.2 The Data Protection Officer is responsible for the monitoring, revision and updating of this policy document on an annual basis or sooner, should the need arise.

9. VALIDITY OF THIS POLICY

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

APPENDIX A

GENERAL DATA PROTECTION REGULATION 2018 - THE DATA PROTECTION PRINCIPLES

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

APPENDIX B

SUMMARY OF RELEVANT LEGISLATION AND GUIDANCE

General Data Protection Regulations (GDPR)

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

Human Rights Act 1998

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

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

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

Freedom of Information Act 2000

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

Regulation of Investigatory Powers Act 2000

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

Crime and Disorder Act 1998

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

The Computer Misuse Act 1990

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

computers for fraudulent activities or other personal gain. Any member of staff found to have contravened this Act will be considered to have committed a disciplinary offence and be dealt with accordingly.

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

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

APPENDIX C

INDIVIDUAL RIGHTS OF THE DATA SUBJECT

1. The Right to be Informed: Individuals have the right to be provided with clear and concise information about what an organisation does with their personal data. NWLDC has published Privacy Notices for each of its departments that outline in detail what data we collect, how that data is used, the lawful basis for processing the data and for how long we will retain that data. These can be found on our website at:

https://www.nwleics.gov.uk/pages/data_protection_notice
2. The Right of Access: Individuals have the right to access their personal data that is held by an organisation (commonly referred to as Subject Access). You have the right to obtain a copy of your personal data by making a Subject Access Request as detailed below.
3. The Right to Rectification: Individuals have the right to have inaccurate personal data rectified, or completed if it is incomplete. You can make a request for rectification as detailed below.
4. The Right to Erasure: Individuals have the right to have their personal data erased or 'forgotten' in certain circumstances. These include when the data is no longer necessary for the purpose in which we originally collected or processed it, when we are relying on your consent to process the data and you choose to withdraw that consent, when we are relying on legitimate interests as our basis for processing and you object to this processing (so long as there is no overriding legitimate interest to continue this processing), we have processed the personal data unlawfully, we have to do it to comply with a legal obligation or we have processed the personal data to offer information society services to a child. The Right to Erasure is not an absolute right and only applies in these circumstances listed; however, we will make every effort to assist you. You can make a request for erasure as detailed below.
5. The Right to Restrict Processing: Individuals have the right to restrict or suppress the processing of their personal data where they have a particular reason for wanting the restriction. This is not an absolute right and only applies in certain circumstances. When processing is restricted, we are permitted to store the data, but not to use it. This right may apply if you are contesting the accuracy of your data and we are verifying that accuracy, if the data has been unlawfully processed and rather than invoking the Right to Erasure you request restriction instead, if we no longer need the personal data but you need NWLDC to keep it in order to establish, exercise or defend a legal claim, or you object to our processing of your data and we are considering whether our legitimate grounds for processing override your request. You can request the restriction of data processing as detailed below.
6. The Right to Data Portability: Individuals have the right to obtain and reuse their personal data for their own purposes across different services. This allows you to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability. You have the right to request that we transfer the data you have provided to NWLDC directly to another Data Controller. This right only applies when the lawful basis for processing the information is consent or for the performance of a contract and we are carrying out the processing by automated means (in other words, it excludes paper files). You can make a data portability request as detailed below.

7. The Right to Object: Individuals have the right to object to the processing of their data in certain circumstances. You have the absolute right to stop your data being used for direct marketing. You may also object to processing if it is for a task carried out in the public interest, the exercise of official authority vested in us or our legitimate interests (or those of a third party); however, the right to object is not absolute in these circumstances. You can make an objection as detailed below.
8. Rights in Relation to Automated Decision Making and Profiling: The GDPR has provisions on making a decision solely by automated means without any human involvement and the automated processing of personal data to evaluate certain things about an individual. All automated decision-making and profiling is subject to the GDPR and NWLDC will identify, when applicable, whether any of our data processing relies solely on automated decision-making or whether we use profiling of any kind. This information is available on our website at:

https://www.nwleics.gov.uk/pages/data_protection_notice

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

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

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

Document Control

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

This page is intentionally left blank

ICT AND CYBER SECURITY POLICY

Version Control

Version No.	Author	Date	Update Information
2.3	Sam Outama	22.06.2020	General review and update
2.2	Sam Outama	30.05.2019	Update to Cyber Security
2.1	Sam Outama	14.09.2017	Update Password Control
2	Sam Outama	25.07.2017	General Update
1.1	Ivan Arkinstall	09.07.2013	Revised
1	Phil Clarke	04.03.2009	Revised

June 2020

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

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

9.1	Compliance with Legal Requirements and Codes of Practice	27
9.1.1	Control of Proprietary Software Copying	27
9.1.2	Use of Unlicensed Software	28
9.1.3	Safeguarding of the Council's Records	28
9.1.4	Auditing and Logging the use of ICT Resources	28
9.1.5	Data Protection	28
9.1.6	Prevention of Misuse of ICT Facilities	29
9.2	Security Review of ICT Systems	30
9.3	System Audit Considerations	30
	Appendices	
	Appendix 1 - The National Protective marking Scheme	31
	The PROTECT Classification	32
	The RESTRICTED Classification	33
	Major Differences Between PROTECT and RESTRICTED	34
	Appendix 2 - GCSx Personal Commitment Statement	36
	Appendix 3 - Third Party Code of Connection	40

ICT AND CYBER SECURITY POLICY

FORWARD

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

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

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

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

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

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

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

POLICY OBJECTIVES

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

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

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

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

The main objectives of this policy are:

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

The strategic approach to cyber security is based on:

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

SCOPE

This Information Technology and Cyber Security Policy will apply to:

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

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

1. SECURITY ORGANISATION

Objective:

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

1.1 Responsibilities

The ICT Manager is responsible for:

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

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

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

Departmental application software is the responsibility of:

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

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

1.2 Acquisition of Information and Communications Technology

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

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

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

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

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

1.3 Security Information Advice

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

1.4 Security Incidents

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

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

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

1.5 Independent Review of Information Security

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

2. **SECURITY OF THIRD PARTY ACCESS**

Objective:

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

2.1 Identification of Risks from Third Party Connections

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

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

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

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

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

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

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

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

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

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

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

3. ASSETS CONTROL

Objective:

To maintain appropriate protection of organisational assets:

3.1 Inventory of Assets

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

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

4. PERSONNEL SECURITY

Objective:

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

4.1 General

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

All potential recruits will be screened by:

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

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

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

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

4.2 ICT and Cyber Security Training

Objective:

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

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

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

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

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

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

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

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

4.3 Responding to Incidents

Objective:

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

A security incident shall mean:

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

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

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

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

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

5. **PHYSICAL AND ENVIRONMENTAL SECURITY**

Objective:

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

5.1 Secure Areas

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

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

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

The following specific conditions will apply to such secure areas:

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

5.2 Equipment Security

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

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

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

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

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

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

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

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

5.3 Equipment and Data Destruction

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

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

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

5.4 Remote Access to Systems and Data

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

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

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

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

Specific conditions and responsibilities will apply to those users:

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

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

6. COMPUTER AND NETWORK MANAGEMENT

6.1 Operational Procedures and Responsibilities

Objective:

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

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

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

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

6.2 System Planning and Acceptance

Objective:

To minimise the risk of systems failure:

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

Acceptance procedures for new systems will include the following:

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

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

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

6.3 Configuration and Change Management

Objective:

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

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

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

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

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

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

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

6.4 Protection from Malicious and Unauthorised Software

Objective:

To safeguard the integrity of software and data:

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

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

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

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

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

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

6.5 Housekeeping

Objective:

To maintain the integrity and availability of IT services:

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

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

Documented procedures for each system shall include:

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

6.6 Network Management

Objective:

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

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

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

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

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

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

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

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

6.7 Media Handling and Security

Objective:

To prevent damage to assets and interruptions to business activities:

Computer media containing data shall be controlled and physically protected.

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

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

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

6.8 Data and Software Exchange

Objective:

To prevent loss, modification or misuse of data:

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

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

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

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

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

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

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

6.9 Connection to Other Networks

Objective:

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

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

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

6.10 Electronic Mail

Objective:

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

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

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

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

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

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

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

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

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

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

6.10.1 Confidential or RESTRICTED Information

Specific conditions apply to the use of RESTRICTED information:

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

6.10.2 Use of E-mail Outside the UK

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

6.11 Internet

Objective:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

7. SYSTEM ACCESS CONTROL

7.1 Business Requirements for System Access

Objective:

To control access to business information:

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

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

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

Domain privileged access will be reviewed periodically.

7.2 User Access Management

Objective:

To prevent unauthorised computer access:

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

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

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

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

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

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

7.3 User Responsibilities

Objective:

To prevent unauthorised computer access:

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

In order to maintain security users must:

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

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

7.4 Network Access Control

Objective:

Protection of networked services:

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

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

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

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

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

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

7.5 Computer and Application Access Control

Objective:

To prevent unauthorised access to computers and information held:

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

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

8. SYSTEMS DEVELOPMENT AND MAINTENANCE

8.1 Security Requirements in Systems

Objective:

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

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

The analysis of security requirements should:

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

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

8.2 Security of Application System Files

Objective:

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

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

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

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

8.3 Security in Development and Support Environments

Objective:

To maintain the security of application systems software and data:

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

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

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

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

9. COMPLIANCE

9.1 Compliance with Legal Requirements and Codes of Practice

Objective:

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

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

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

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

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

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

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

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

9.1.1 Control of Proprietary Software Copying

Objective:

To ensure that the Council complies with current legislation:

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

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

9.1.2 Use of Unlicensed Software

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

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

9.1.3 Safeguarding of the Council's Records

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

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

9.1.4 Auditing and logging the use of ICT resources

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

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

9.1.5 Data Protection

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

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

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

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

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

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

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

9.1.6 Prevention of Misuse of IT Facilities

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

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

The following conditions will apply:

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

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

9.2 Security Reviews of IT Systems

Objective:

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

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

This will be carried out by an approved CREST/IASME

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

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

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

9.3 System Audit Considerations

Objective:

To minimise interference to / from the system audit process:

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

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

The following are to be observed:

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

Access to system audit tools should be controlled.

THE NATIONAL PROTECTIVE MARKING SCHEME FRAMEWORK

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

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

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

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

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

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

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

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

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

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

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

The PROTECT Classification

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

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

The RESTRICTED Classification

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

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

Major Differences Between PROTECT and RESTRICTED

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

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

***SIGN BELOW TO ACCEPT THE ICT SECURITY POLICY AND HAND
THE FORM TO THE ICT DEPARTMENT***

**North West Leicestershire District Council
Information and Communications Technology (ICT) and Cyber
Security Policy**

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

It follows that a high standard of information security is required within the Council. To achieve this, the ICT and Cyber Security Policy has been adopted and everyone who uses IT equipment or accesses Council information must read the policy and ensure that they understand the obligations contained within it.

Once you have **read** and **understood** the ICT and Cyber Security Policy please sign and return the slip below to the ICT Service Desk.

North West Leicestershire District Council ICT and Cyber Security and Policy can be found on our intranet site

✂-----✂

**North West Leicestershire District Council
Information and Communications Technology (ICT) and Cyber
Security Policy**

I have read and understand the North West Leicestershire District Council's ICT Security Policy.

Print Name _____ Signed _____ Date _____

(Note: When completed, this should be forwarded to the IT Section, who will copy it to the Human Resources Section)

**NORTH WEST LEICESTERSHIRE DISTRICT COUNCIL -
GCSx PERSONAL COMMITMENT STATEMENT**

I understand and agree to comply with the security rules of my organisation as well as the GCSx Code of Connection.

For the avoidance of doubt, the security rules relating to secure e-mail and IT systems usage include:

1. I acknowledge that my use of the GCSx may be monitored and/or recorded for lawful purposes.
2. I agree to be responsible for any use by me of the GCSx using my unique user credentials (user ID and password, access token or other mechanism as provided) and e-mail address.
3. I will not use a colleague's credentials to access the GCSx and will equally ensure that my credentials are not shared and are protected against misuse.
4. I will protect such credentials at least to the same level of secrecy as the information they may be used to access, (in particular, I will not write down or share my password other than for the purposes of placing a secured copy in a secure location at my employer's premises).
5. I will not attempt to access any computer system that I have not been given explicit permission to access.
6. I will not attempt to access the GCSx other than from IT systems and locations which I have been explicitly authorised to use for this purpose.
7. I will not transmit information via the GCSx that I know, suspect or have been advised is of a higher level of sensitivity than my GCSx domain is designed to carry.
8. I will not transmit information via the GCSx that I know or suspect to be unacceptable within the context and purpose for which it is being communicated.
9. I will not make false claims or denials relating to my use of the GCSx (e.g. falsely denying that an e-mail had been sent or received).
10. I will protect any sensitive or not protectively marked material sent, received, stored or processed by me via the GCSx to the same level as I would paper copies of similar material.
11. I will not send Protectively Marked information over public networks such as the Internet.
12. I will always check that the recipients of e-mail messages are correct so that potentially sensitive or protectively marked information is not accidentally released into the public domain.
13. I will not auto-forward e-mail from my GCSx account to any other non-GCSx e-mail account.

14. I will disclose information received via the GCSx only on a 'need to know' basis.
15. I will not forward or disclose any sensitive or protectively marked material received via the GCSx unless the recipient(s) can be trusted to handle the material securely according to its sensitivity and forwarding is via a suitably secure communication channel.
16. I will seek to prevent inadvertent disclosure of sensitive or protectively marked information by avoiding being overlooked when working, by taking care when printing information received via the GCSx (e.g. by using printers in secure locations or collecting printouts immediately they are printed, checking that there is no interleaving of printouts, etc) and by carefully checking the distribution list for any material to be transmitted.
17. I will securely store or destroy any printed material.
18. I will not leave my computer unattended in such a state as to risk unauthorised disclosure of information sent or received via the GCSx (this might be by closing the e-mail program, logging-off from the computer, activate a password-protected screensaver, etc, so as to require a user logon for activation).
19. Where my organisation has implemented other measures to protect unauthorised viewing of information displayed on IT systems (such as an inactivity timeout that causes the screen to be blanked or to display a screensaver or similar, requiring a user logon for reactivation), then I will not attempt to disable such protection.
20. I will make myself familiar with the security policies, procedures and any special instructions that relate to the GCSx.
21. I will inform my manager immediately if I detect, suspect or witness an incident that may be a breach of security.
22. I will not attempt to bypass or subvert system security controls or to use them for any purpose other than that intended.
23. I will not remove equipment or information from my employer's premises without appropriate approval.
24. I will take precautions to protect all computer media and portable computers when carrying them outside my organisation's premises (e.g. leaving a laptop unattended or on display in a car such that it would encourage an opportunist thief).
25. I will not introduce viruses, Trojan horses or other malware into the system or GCSx.
26. I will comply with the Data Protection Act 1998 and any other legal, statutory or contractual obligations that my employer informs me are relevant.
27. If I am about to leave my employer, I will inform my manager prior to departure of any important information held in my account.
28. The GCSx Acceptable Usage Policy specifically states that all PROTECT and RESTRICT information will be appropriately labelled when sent over the GCSx and that public networks will not be used to send RESTRICT or PROTECT information.

29. I understand that use of GCSx / PSN services is subjected to Criminal conviction checks and I will declare any unspent convictions including cautions, reprimands, warnings, investigations or pending prosecutions to Human Resources.

**PLEASE SIGN BELOW TO ACCEPT THE GCSx SECURITY POLICY
AND HAND THE FORM TO THE ICT DEPARTMENT**

Name: Dept:

Signed: Date:

Authorised: Date:

This form can only be authorised by Team Managers or members of
CLT.

**(Note: When completed, this should be forwarded to the IT Section, who will copy it to
the Human Resources Section)**

THIRD PART NETWORK ACCESS AGREEMENT

1. Purpose

The purpose of this agreement is to outline the specific terms and conditions governing the access and use of the North West Leicestershire District Council (NWLDC) network and information technology resources by the Third Party.

This agreement is dated and made between **North West Leicestershire District Council** and the following Third Party:

Company name:	[]
Address:	[]
	[]
	[]
Contact Name:	[]
Phone number:	[]
E-mail address:	[]

2. Definitions

Third parties are defined as any individual, consultant, contractor, vendor or agent not registered as a NWLDC employee.

Third party access is defined as all local or remote access to the NWLDC network for any purpose.

NWLDC network includes all data, applications, systems, services, infrastructure and computer devices which are owned or leased by the NWLDC.

Mobile computer devices are defined as any handheld computer device, including but not limited to laptops, notebooks, tablet computers, smartphone devices (e.g. PDA, iPhone and Blackberry enabled devices, etc).

Removable storage devices are defined as any optical or magnetic storage device or media, including but not limited to floppy disks, CD, DVD, magnetic tapes, ZIP disk, USB flash drive (i.e. memory stick / pen / keys), external / portable hard drives and SD Cards.

3. Terms and Conditions

In consideration of NWLDC engaging the Third Party for services requiring third party access and allowing such third party access, the Third Party agrees to the following:

- (a) The Third Party may only use the network connection for approved business purposes as specified by NWLDC and in accordance with NWLDC ICT policies. The use of the network connection for unapproved purposes, including but not limited to personal use or gain is strictly prohibited.
- (b) The Third Party may only use access methods which have been defined by the NWLDC ICT Services.

- (c) The Third Party must ensure that only their employees that have been nominated by the Third Party and approved by the NWLDC in advance, have access to the network connection or any NWLDC owned equipment.
- (d) The Third Party shall be solely responsible for ensuring its nominated employees are not security risks, and upon request from the NWLDC, the Third Party will provide the NWLDC with any information reasonably necessary for the NWLDC to evaluate security issues.
- (e) The Third Party will promptly inform the NWLDC in writing of any relevant employee changes. This includes the rotation and resignation of employees so that NWLDC can disable their usernames and remove / change passwords in order to secure its resources.
- (f) As part of any service agreement review the Third Party will provide the NWLDC with an up to date list of their employees who have access to the network connection or any NWLDC owned equipment.
- (g) The Third Party is solely responsible for ensuring that all usernames and passwords issued to them by the NWLDC remain confidential and are not used by unauthorised individuals. The Third Party must immediately contact NWLDC if they suspect these details have been compromised.
- (h) The Third Party will be held responsible for all activities performed on the NWLDC network while logged in under their usernames and passwords.
- (i) The Third Party must ensure at all times that all computer devices used by them to connect to the NWLDC network have reputable up to date anti-virus software and the appropriate security patches installed.
- (j) Only in exceptional circumstances and with the prior written approval of the NWLDC should the Third Party hold NWLDC information on mobile computer devices or removable storage devices. Should the business requirements necessitate the Third Party to store NWLDC information on mobile computer devices or removable storage devices, the Third Party must ensure that only the absolute minimum amount of information as is absolutely necessary is stored on the mobile computer device or removable storage device and the information is securely deleted when it is no longer required. The Third Party must ensure that all NWLDC information stored on mobile computer devices and removable storage devices belonging to the Third Party is encrypted to standards approved by NWLDC. Under no circumstance encrypted or otherwise should NWLDC information be stored by the Third Party on USB memory keys / sticks.
- (k) The Third Party must ensure that all mobile computer devices used by them to connect to the NWLDC network, are used in such a way that information belonging to the NWLDC is not displayed to unauthorised individuals or the general public.
- (l) The Third Party must ensure that all their computer devices connected to the NWLDC network are not connected to any other network at the same time, with the exception of networks that are under the complete control of the Third Party.
- (m) When the Third Party is connected to the NWLDC network they should not leave their computer devices unattended.

- (n) The Third Party must ensure that when they are connected to NWLDC network their activity does not disrupt or interfere with other non-related network activity.
- (o) All Third Party computer devices used to connect to the NWLDC network must, upon request by NWLDC be made available for inspection.
- (p) The Third Party network connection will by default be granted read / execute privileges only. All requests for increased privileges must be submitted in writing to the NWLDC where they will be considered on a case by case basis.
- (q) For security reasons all Third Party remote access accounts except those providing 24*7 support may be switched off (de-activated) by default. The Third Party will be required to e-mail (can be followed by phone) NWLDC ICT Services requesting that their account be switched-on (activated) for a stipulated period.
- (r) The Third Party must obtain the written consent of the NWLDC before implementing any updates or amendments to the NWLDC network, information systems, applications or equipment. All approved updates and amendments implemented by the Third Party must be made in line with NWLDC policies and procedures.
- (s) The Third Party must ensure all software is scanned and cleared of all viruses and other forms of malicious software before it is installed on any NWLDC information systems, applications or equipment. The Third Party will be held responsible for all disruptions and damage caused to the NWLDC network, information systems, applications or equipment which is traced back to infected software installed by the Third Party.
- (t) The Third Party and their employees must comply with all UK, European and NWLDC rules and regulations concerning safety, environmental and security operations while on-site at an NWLDC site. All Third Party personnel must carry photographic identification with them when they are on-site at an NWLDC facility.
- (u) Where the Third Party has direct or indirect access to NWLDC information, this information must not be copied, divulged or distributed to any other party without the prior written approval of the NWLDC.
- (v) The Third Party must report all actual and suspected security incidents to the NWLDC immediately.
- (w) The Third Party must manage and process all NWLDC information which they acquire from the NWLDC in accordance the Data Protection Act 1998 (as amended or replace) and any associated guidance.
- (x) The NWLDC reserves the right to:
 - Monitor all Third Party activity while connected (local and remote) to the NWLDC network.
 - Audit contractual responsibilities or have those audits carried out by an NWLDC approved third party
 - Revoke the Third Party's access privileges at any time.
- (y) On completion of the services requiring third party access, the Third Party must return all equipment, software, documentation and information belonging to the NWLDC.

- (z) Any violations of this agreement by the Third Party, may lead to the withdrawal of NWLDC network and information technology resources to that Third Party and/or the cancellation of any contract(s) between the NWLDC and the Third Party.

The Third Party agrees to abide by the terms and conditions of this agreement at all times.

Signed (On behalf of the Third Party):

Authorised Signature:

Name (Printed):

Title or Position:

Date:

This page is intentionally left blank

LOCAL CODE OF CORPORATE GOVERNANCE

Policy Statement

Version Control

Version No.	Author	Date
1		2009
2	Tracy Bingham	October 2017
3	Tracy Bingham	May 2020

May 2020

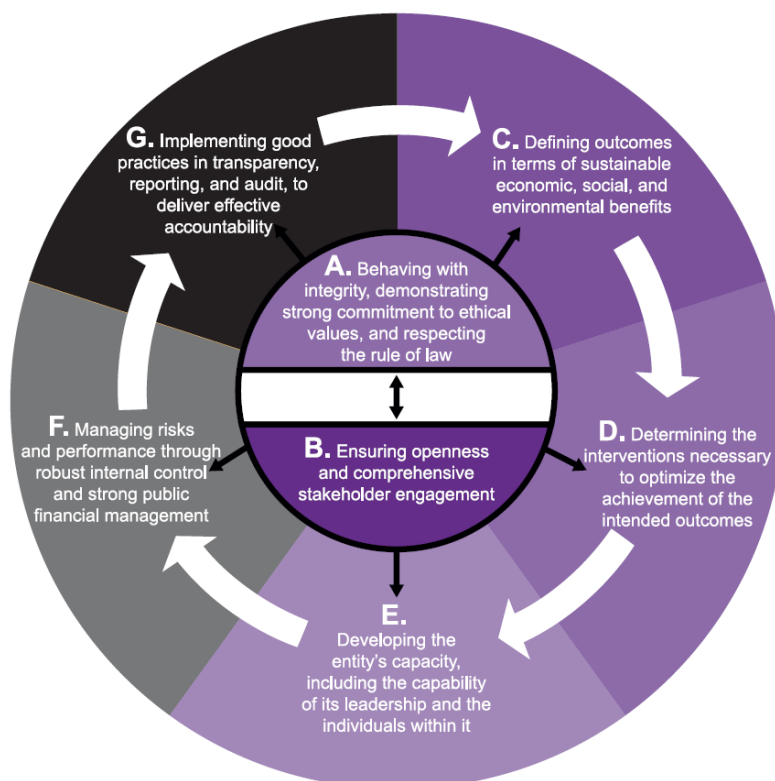
	Contents	Page No.
1.	Introduction	3
2.	Summary of Commitment	4
3.	Fundamental Principles of Corporate Governance	4

NORTH WEST LEICESTERSHIRE DISTRICT COUNCIL Local Code of Corporate Governance

1 INTRODUCTION

- 1.1 In 2014, the Chartered Institute of Public Finance and Accountancy (CIPFA) and the International Federation of Accountants (IFAC) collaborated to produce The International Framework: Good Governance in the Public Sector. The International Framework defines governance as comprising the arrangements put in place to ensure that intended outcomes for stakeholders are defined and achieved. It states that in order to deliver good governance in the public sector, both governing bodies and individuals working for public sector entities must try to achieve their entity's objectives while acting in the public interest at all times.
- 1.2 The Chartered Institute of Public Finance and Accountancy in association with SOLACE have published their Framework entitled 'Delivering Good Governance in Local Government 2016'.
- 1.3 The diagram below¹ illustrates the core principles of good governance in the public sector and how they relate to each other: Principles A and B permeates implementation of principles C to G.

Achieving the Intended Outcomes While Acting in the Public Interest at all Times



¹ CIPFA/SOLACE Delivering Good Governance in Local Government Framework 2016

- 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).

2 SUMMARY OF COMMITMENT

- 2.1 By adopting this Local Code of Corporate Governance, we are responding to the CIPFA/SOLACE Joint Working Group Guidance and Framework entitled 'Delivering Good Governance in Local Government'.
- 2.2 In doing so we will:
 - Accept the core principles set out in section 3 below as the basis for our Corporate Governance arrangements.
 - Publish an Annual Governance Assurance Statement with the Council's Statement of Accounts.
 - Draw up Action Plans of improvements to our corporate governance arrangements, such plans to be monitored by the Audit and Governance Committee.

3 FUNDAMENTAL PRINCIPLES OF CORPORATE GOVERNANCE

- 3.1 Set out in this document is the Council's proposed Local Code of Corporate Governance which is based on the seven core principles (as set out in the illustration above) adopted for local government from the report of the Independent Commission on Good Governance in Public Services.

Principle A - Behaving with integrity, demonstrating strong commitment to ethical values, and respecting the rule of law

The Council is committed to:

Behaving with Integrity

- Ensuring members and officers behave with integrity and lead as a culture where acting in the public interest is visibly and consistently demonstrated thereby protecting the reputation of the organisation.
- Ensuring members take the lead in establishing specific standard operating principles or values for the organisation and its staff and that they are communicated and understood. These should build on the Seven Principles of Public Life (The Nolan Principles).
- Leading by example and using these standard operating principles or values as a framework for decision making and other actions.
- Demonstrating, communicating and embedding the standard operating principles or values through appropriate policies and processes which are reviewed on a regular basis to ensure they are operating effectively.

Demonstrating strong commitment and ethical values

- Seeking to establish, monitor and maintain the organisation's ethical standards and performance
- Underpinning personal behaviour with ethical values and ensuring they permeate all aspects of the organisation's culture and operation
- Developing and maintaining robust policies and procedures which place emphasis on agreed ethical values
- Ensuring that external providers of services on behalf of the organisation are required to act with integrity and in compliance with high ethical standards expected by the organisation

Respecting the rule of law

- Ensuring members and staff demonstrate a strong commitment to the rule of the law as well as adhering to relevant laws and regulations
- Creating the conditions to ensure that the statutory officers, other key post holders and members are able to fulfil their responsibilities in accordance with legislative and regulatory requirements
- Striving to optimise the use of the full powers available for the benefit of citizens, communities and other stakeholders
- Dealing with breaches of legal and regulatory provisions effectively
- Ensuring corruption and misuse of power are dealt with effectively

Principle B – Ensuring openness and comprehensive stakeholder engagement

The Council is committed to:

Openness

- Ensuring an open culture through demonstrating, documenting and communicating the organisation's commitment to openness
- Making decisions that are open about actions, plans, resource use, forecasts, outputs and outcomes. The presumption is for openness. If that is not the case, a justification for the reasoning for keeping a decision confidential should be provided
- Providing clear reasoning and evidence for decisions in both public records and explanations to stakeholders and being explicit about the criteria, rationale and considerations used. In due course, ensuring that the impact and consequences of those decisions are clear
- Using formal and informal consultation and engagement to determine the most appropriate and effective interventions/ courses of action

Engaging comprehensively with institutional stakeholders

- Effectively engaging with institutional stakeholders to ensure that the purpose, objectives and intended outcomes for each stakeholder relationship are clear so that outcomes are achieved successfully and sustainably
- Developing formal and informal partnerships to allow for resources to be used more efficiently and outcomes achieved more effectively
- Ensuring that partnerships are based on: trust, a shared commitment to change, a culture that promotes and accepts challenge among partners and that the added value of partnership working is explicit

Engaging stakeholders effectively, including individual citizens and service users

- Establishing a clear policy on the type of issues that the organisation will meaningfully consult with or involve individual citizens, service users and other stakeholders to ensure that service (or other) provision is contributing towards the achievement of intended outcomes.
- Ensuring that communication methods are effective and that members and officers are clear about their roles with regard to community engagement
- Encouraging, collecting and evaluating the views and experiences of communities, citizens, service users and organisations of different backgrounds including reference to future needs
- Implementing effective feedback mechanisms in order to demonstrate how their views have been taken into account
- Balancing feedback from more active stakeholder groups with other stakeholder groups to ensure inclusivity
- Taking account of the interests of future generations of tax payers and service users

Principle C – Defining outcomes in terms of sustainable economic, social, and environmental benefits

The Council is committed to:

Defining outcomes

- Having a clear vision which is an agreed formal statement of the organisation's purpose and intended outcomes containing appropriate performance indicators, which provides the basis for the organisation's overall strategy, planning and other decisions
- Specifying the intended impact on, or changes for, stakeholders including citizens and service users. It could be immediately or over the course of a year or longer
- Delivering defined outcomes on a sustainable basis within the resources that will be available
- Identifying and managing risks to the achievement of outcomes
- Managing service users expectations effectively with regard to determining priorities and making the best use of the resources available

Sustainable economic, social and environmental benefits

- Considering and balancing the combined economic, social and environmental impact of policies, plans and decisions when taking decisions about service provision
- Taking a longer-term view with regard to decision making, taking account of risk and acting transparently where there are potential conflicts between the organisation's intended outcomes and short-term factors such as the political cycle or financial constraints
- 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
- Ensuring fair access to services

Principle D – Determining the interventions necessary to optimise the achievement of the intended outcomes

The Council is committed to:

Determining interventions

- Ensuring decision makers receive objective and rigorous analysis of a variety of options indicating how intended outcomes would be achieved and including the risks associated with those options. Therefore ensuring best value is achieved however services are provided
- Considering feedback from citizens and service users when making decisions about service improvements or where services are no longer required in order to prioritise competing demands within limited resources available including people, skills, land and assets and bearing in mind future impacts

Planning interventions

- Establishing and implementing robust planning and control cycles that cover strategic and operational plans, priorities and targets
- Engaging with internal and external stakeholders in determining how services and other courses of action should be planned and delivered
- Considering and monitoring risks facing each partner when working collaboratively including shared risks
- Ensuring arrangements are flexible and agile so that the mechanisms for delivering outputs can be adapted to changing circumstances
- Establishing appropriate key performance indicators (KPIs) as part of the planning process in order to identify how the performance of services and projects is to be measured
- Ensuring capacity exists to generate the information required to review service quality regularly
- Preparing budgets in accordance with organisational objectives, strategies and the medium term financial plan Informing medium and long term resource planning by drawing up realistic estimates of revenue and capital expenditure aimed at developing a sustainable funding strategy

Optimising achievement of intended outcomes

- Ensuring the medium term financial strategy integrates and balances service priorities, affordability and other resource constraints
- Ensuring the budgeting process is all-inclusive, taking into account the full cost of operations over the medium and longer term
- Ensuring the medium term financial strategy sets the context for ongoing decisions on significant delivery issues or responses to changes in the external environment that may arise during the budgetary period in order for outcomes to be achieved while optimising resource usage
- Ensuring the achievement of 'social value' through service planning and commissioning.

Principle E – Developing the entity’s capacity, including the capability of its leadership and the individuals within it

The Council is committed to:

Developing the entity’s capacity

- Reviewing operations, performance use of assets on a regular basis to ensure their continuing effectiveness
- Improving resource use through appropriate application of techniques such as benchmarking and other options in order to determine how the authority’s resources are allocated so that outcomes are achieved effectively and efficiently
- Recognising the benefits of partnerships and collaborative working where added value can be achieved
- Developing and maintaining an effective workforce plan to enhance the strategic allocation of resources

Developing the capability of the entity’s leadership and other individuals

- Developing protocols to ensure that elected and appointed leaders negotiate with each other regarding their respective roles early on in the relationship and that a shared understanding of roles and objectives is maintained
- Publishing a statement that specifies the types of decisions that are delegated and those reserved for the collective decision making of the governing body
- Ensuring the leader and the chief executive have clearly defined and distinctive leadership roles within a structure whereby the chief executive leads the authority in implementing strategy and managing the delivery of services and other outputs set by members and each provides a check and a balance for each other’s authority
- Developing the capabilities of members and senior management to achieve effective shared leadership and to enable the organisation to respond successfully to changing legal and policy demands as well as economic, political and environmental changes and risks by:
 - ensuring members and staff have access to appropriate induction tailored to their role and that ongoing training and development matching individual and organisational requirements is available and encouraged
 - ensuring members and officers have the appropriate skills, knowledge, resources and support to fulfil their roles and responsibilities and ensuring that they are able to update their knowledge on a continuing basis
 - ensuring personal, organisational and system-wide development through shared learning, including lessons learnt from governance weaknesses both internal and
- Ensuring that there are structures in place to encourage public participation
- Taking steps to consider the leadership’s own effectiveness and ensuring leaders are open to constructive feedback from peer review and inspections
- Holding staff to account through regular performance reviews which take account of training or development needs Ensuring arrangements are in place to maintain the health and wellbeing of the workforce and support individuals in maintaining their own physical and mental wellbeing

Principle F – Managing risks and performance through robust internal control and strong public financial management

The Council is committed to:

Managing risk

- Recognising that risk management is an integral part of all activities and must be considered in all aspects of decision making
- Implementing robust and integrated risk management arrangements and ensuring that they are working effectively
- Ensuring that responsibilities for managing individual risks are clearly allocated

Managing performance

- Monitoring service delivery effectively including planning, specification, execution and independent post implementation review
- Making decisions based on relevant, clear objective analysis and advice pointing out the implications and risks inherent in the organisation's financial, social and environmental position and outlook
- Ensuring an effective scrutiny or oversight function is in place which encourages constructive challenge and debate on policies and objectives before, during and after decisions are made thereby enhancing the organisation's performance and that of any organisation for which it is responsible (OR, for a committee system) Encouraging effective and constructive challenge and debate on policies and objectives to support balanced and effective decision making
- Providing members and senior management with regular reports on service delivery plans and on progress towards outcome achievement
- Ensuring there is consistency between specification stages (such as budgets) and post implementation reporting (e.g. financial statements)

Robust internal control

- Aligning the risk management strategy and policies on internal control with achieving the objectives
- Evaluating and monitoring the authority's risk management and internal control on a regular basis
- Ensuring effective counter fraud and anti-corruption arrangements are in place
- Ensuring additional assurance on the overall adequacy and effectiveness of the framework of governance, risk management and control is provided by the internal auditor
- Ensuring an audit committee or equivalent group or function which is independent of the executive and accountable to the governing body: provides a further source of effective assurance regarding arrangements for managing risk and maintaining an effective control environment that its recommendations are listened to and acted upon

Managing Data

- Ensuring effective arrangements are in place for the safe collection, storage, use and sharing of data, including processes to safeguard personal data
- Ensuring effective arrangements are in place and operating effectively when sharing data with other bodies
- Reviewing and auditing regularly the quality and accuracy of data used in decision making and performance monitoring

Strong public financial management

- Ensuring financial management supports both long term achievement of outcomes and short-term financial and operational performance
- Ensuring well-developed financial management is integrated at all levels of planning and control, including management of financial risks and controls

Principle G – Implementing good practices in transparency, reporting, and audit to deliver effective accountability

The Council is committed to:

Implementing good practice in transparency

- Writing and communicating reports for the public and other stakeholders in an understandable style appropriate to the intended audience and ensuring that they are easy to access and interrogate
- Striking a balance between providing the right amount of information to satisfy transparency demands and enhance public scrutiny while not being too onerous to provide and for users to understand

Implementing good practice in reporting

- Reporting at least annually on performance, value for money and the stewardship of its resources
- Ensuring members and senior management own the results
- Ensuring robust arrangements for assessing the extent to which the principles contained in the Framework have been applied and publishing the results on this assessment including an action plan for improvement and evidence to demonstrate good governance (annual governance statement)
- Ensuring that the Framework is applied to jointly managed or shared service organisations as appropriate
- Ensuring the performance information that accompanies the financial statements is prepared on a consistent and timely basis and the statements allow for comparison with other similar organisations

Assurance and effective accountability

- Ensuring that recommendations for corrective action made by external audit are acted upon
- Ensuring an effective internal audit service with direct access to 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

- 4.1 The contents of this Local Code will be reviewed when necessary usually on an annual basis.

NWLDC

REVIEWED AND UPDATED – FEBRUARY 2008

REVIEWED – JUNE 2009

REVIEWED AND UPDATED – SEPTEMBER 2017

This page is intentionally left blank

Title of Report	STANDARDS AND ETHICS - QUARTER 3 REPORT	
Presented by	Head of Legal and Commercial Services and Monitoring Officer 01530 454762 Elizabeth.warhurst@nwleicestershire.gov.uk	
Background Papers	None	Public Report: Yes
Purpose of Report	To receive the figures for local determination of complaints and the ethical indicators for Quarter 3 of 2019/2020	
Recommendations	THE REPORT BE RECEIVED AND NOTED.	

1.0 BACKGROUND

- 1.1 The Standards and Ethics Report provides information in two categories: Local Determination of Complaints and Ethical Indicators.
- 1.2 The Quarter 3 Report follows the revised format and includes commentary where there is a variation in trends reported

Policies and other considerations, as appropriate	
Council Priorities:	Our communities are safe, healthy and connected
Policy Considerations:	N/A
Safeguarding:	Safeguarding in relation to Modern Slavery
Equalities/Diversity:	N/A
Customer Impact:	Customers have the opportunity to report on measures that are included in this report.
Economic and Social Impact:	N/A
Environment and Climate Change:	N/A
Consultation/Community Engagement:	Customers have the opportunity to report on measures that are included in this report
Risks:	By receiving this information members will be able to manage risks.
Officer Contact	Elizabeth Warhurst Head of Legal and Commercial Services elizabeth.warhurst@nwleicestershire.gov.uk

Standards and Ethics

Quarter 3 Report

2019-2020

Contents

Page 1 - Introduction

Page 2 - Local Determinations of Complaints

Page 3 - Ethical Indicators

Page 4 - Freedom of Information Requests

Page 5 - Definitions

Introduction

This is the quarterly report to the Audit & Governance Committee detailing both the figures for the Ethical Indicators and the figures for the Local Determination of Complaints process for 2019/20.

For clarification purposes the months covered by the quarters are as follows:

Quarter 1 - 1 April to 30 June

Quarter 2 - 1 July to 30 September

Quarter 3 - 1 October to 31 December

Quarter 4 - 1 January to 31 March

The report is split into 2 parts for ease of reference; Part 1 refers to the local determination of complaints, part 2 is the table showing the ethical indicators figures.

The report will enable the Audit & Governance Committee to build up a picture over time of how many complaints are received and where these are coming from. The parts of the Code of Conduct which have been breached will also be recorded to enable training to be targeted effectively.

Local Determination of Complaints

The Monitoring Officer received 0 complaints in Quarter 3 of 2019/20.

2.1 Assessment Sub-committee Decisions

There has been no Assessment Sub-committee meetings in this quarter.

The Monitoring Officer pursues an informal dispute resolution process prior to initiating formal proceedings via the Sub-committee route.

One complaint received in Quarter 2 has been resolved informally in Quarter 3.

2.2 Timeliness of Decision

The Standards for England Guidance stated that the Assessment Sub-committee should complete its initial assessment of an allegation “within an average of 20 working days” to reach a decision on what should happen with the complaint. The Council has taken this standard and adapted it under the new rules to aim to hold an Assessment Sub-committee within 20 working days of notifying the parties that informal resolution is not possible.

2.3 Review Requests

There have been no review requests in Quarter 3. Review requests can only be made following a decision of ‘No further Action’ by the Assessment Sub-committee where there is submission of new evidence or information by the complainant.

2.4 Subsequent Referrals

None to report – see above.

2.5 Outcome of Investigations

There were no investigations concluded in this period.

2.6 Parts of the Code Breached

This section is intended to show where there are patterns forming to enable the Audit and Governance Committee to determine where there needs to be further training for Councillors. Targeting training in this way makes it more sustainable and, hopefully, more effective.

So far this year, the following areas of the code were found to have been breached:

N/A

Ethical Indicators

PERFORMANCE INDICATOR	Q1		Q2		Q3		Q4	
	18/19	19/20	18/19	19/20	18/19	19/20	18/19	19/20
Instances of concerns raised re Modern Slavery	n/a	1	n/a	1	n/a	0	n/a	
Instances of concerns raised re Modern Slavery referred to national agencies	n/a	1	n/a	1	n/a	0	n/a	
Number of whistle blowing incidents reported	0	0	0	0	0	0		
Number of Challenges to procurements	n/a	0	n/a	0	n/a	0	n/a	
Public interest Reports	0	0	0	0	0	0		
Objections to the Councils Accounts	0	0	0	0	0	0		
Disciplinary action relating to breaches of the Member/Officer Protocol	0	0	0	0	0	0		
Follow up action relating to breaches of the Member/Officer Protocol	0	0	0	0	0	0		

Freedom of Information Requests

	Q1		Q2		Q3		Q4	
	18/19	19/20	18/19	19/20	18/19	19/20	18/19	19/20
Total Number (FOIs)	43	84	57	100	69	79	109	
% answered on time	84%	99%	96%	95.8%	100%	99%	91%	
Average per month	14	28	19	33	23	26	36	
Average response time (days)	12	11	9	10	11	10	10	
Business as usual (BAUs)	58	59	86	73	55	62	73	
Transfers (TFRs)	29	18	32	22	32	30	42	
Subject access requests (SARs)	3	2	3	12	2	6	7	
Non-compliant requests	0	0	2	0	0	0	0	
Appeals	0	0	0	0	0	0	0	
Withheld due to exemption/fees	7	6	11	18	5	7	10	
Environmental Information Requests - Land Charges Searches (personal)	40	437	47	367	5	308		

- Fewest number of FOI requests received for 19/20, though by a small margin, likely insignificant.

- Average response time remains consistent. Typical response time for Q3 19/20 is two weeks.

- Significantly less exemptions applied at the FOI level compared to Q2 19/20, however new data shows that 19 exemptions were granted to requests handled as business as usual in this period.

- Decreasing number of EIR requests is likely linked to the recent period of uncertainty leading up to the election and generally surrounding Brexit. Reduced investment in land and property results fewer requests for land information. Notably, as of 13/02/2020, the council has already received more EIR requests in 2020 than Q3 19/20.

Definitions

Business as usual Information requested can be sent quickly and easily within the normal course of business

Land Charges specific information about a particular property

Ombudsman Complaint a customer has followed Stage 1 and 2 complaints procedure but unhappy with the outcome they are entitled to take complaint to the Local government Ombudsman who will decide if the Council has a case to answer.

Subject Access Request a request by an individual to see information an organisation holds on them

Transfers requests received that fall out of our remit i.e. Adult social Care or Highways

Environmental Information Request a right for any person to request access to environmental information held by public authorities.

This page is intentionally left blank

NORTH WEST LEICESTERSHIRE DISTRICT COUNCIL

AUDIT AND GOVERNANCE COMMITTEE – WEDNESDAY,
22 JULY 2020



Title of Report	STANDARDS AND ETHICS – QUARTER 4 REPORT	
Presented by	Elizabeth Warhurst Head of Legal and Commercial Services	
Background Papers	None	Public Report: Yes
Purpose of Report	To receive the figures for local determination of complaints and the ethical indicators for Quarter 4 of 2019/2020	
Recommendations	THE REPORT BE RECEIVED AND NOTED.	

1. BACKGROUND

- 1.1 The Standards and Ethics Report provides information in two categories: Local Determination of Complaints and Ethical Indicators.
- 1.2 Following endorsement of the revised format Quarter 4 sees the fourth issue of the new Standards and Ethics Report.

Policies and other considerations, as appropriate	
Council Priorities:	- Our communities are safe, healthy and connected
Policy Considerations:	N/A
Safeguarding:	Safeguarding in relation to Modern Slavery
Equalities/Diversity:	N/A
Customer Impact:	Customers have the opportunity to report on measures that are included in this report.
Economic and Social Impact:	Detail any economic or social impact as a result of the decision.
Environment and Climate Change:	N/A
Consultation/Community Engagement:	Customers have the opportunity to report on measures that are included in this report
Risks:	By receiving this information members will be able

	to manage risks
Officer Contact	Elizabeth Warhurst Head of Legal and Commercial Services elizabeth.warhurst@nwleicestershire.gov.uk

Standards and Ethics

Quarter 4 Report

2019-2020

Contents

Page 1 - Introduction

Page 2 - Local Determinations of Complaints

Page 3 - Ethical Indicators

Page 4 - Freedom of Information Requests

Page 5 - Definitions

Introduction

This is the quarterly report to the Audit & Governance Committee detailing both the figures for the Ethical Indicators and the figures for the Local Determination of Complaints process for 2019/20.

For clarification purposes the months covered by the quarters are as follows:

Quarter 1 - 1 April to 30 June

Quarter 2 - 1 July to 30 September

Quarter 3 - 1 October to 31 December

Quarter 4 - 1 January to 31 March

The report is split into 2 parts for ease of reference; Part 1 refers to the local determination of complaints, part 2 is the table showing the ethical indicators figures.

The report will enable the Audit & Governance Committee to build up a picture over time of how many complaints are received and where these are coming from. The parts of the Code of Conduct which have been breached will also be recorded to enable training to be targeted effectively.

Local Determination of Complaints

The Monitoring Officer received 0 complaints in Quarter 4 of 2019/20.

2.1 Assessment Sub-committee Decisions

There has been no Assessment Sub-committee meetings in this quarter.

The Monitoring Officer pursues an informal dispute resolution process prior to initiating formal proceedings via the Sub-committee route.

0 complaints have been resolved informally in Quarter 4.

2.2 Timeliness of Decision

The Standards for England Guidance stated that the Assessment Sub-committee should complete its initial assessment of an allegation “within an average of 20 working days” to reach a decision on what should happen with the complaint. The Council has taken this standard and adapted it under the new rules to aim to hold an Assessment Sub-committee within 20 working days of notifying the parties that informal resolution is not possible.

2.3 Review Requests

There have been no review requests in Quarter 4. Review requests can only be made following a decision of ‘No further Action’ by the Assessment Sub-committee where there is submission of new evidence or information by the complainant.

2.4 Subsequent Referrals

None to report – see above.

2.5 Outcome of Investigations

There were no investigations concluded in this period.

2.6 Parts of the Code Breached

This section is intended to show where there are patterns forming to enable the Audit and Governance Committee to determine where there needs to be further training for Councillors. Targeting training in this way makes it more sustainable and, hopefully, more effective.

So far this year, the following areas of the code were found to have been breached:

N/A

Ethical Indicators

PERFORMANCE INDICATOR	Q1		Q2		Q3		Q4	
	18/19	19/20	18/19	19/20	18/19	19/20	18/19	19/20
Instances of concerns raised re Modern Slavery	n/a	1	n/a	1	n/a	0	n/a	0
Instances of concerns raised re Modern Slavery referred to national agencies	n/a	1	n/a	1	n/a	0	n/a	0
Number of whistle blowing incidents reported	0	0	0	0	0	0		0
Number of Challenges to procurements	n/a	0	n/a	0	n/a	0	n/a	0
Public interest Reports	0	0	0	0	0	0		0
Objections to the Councils Accounts	0	0	0	0	0	0		0
Disciplinary action relating to breaches of the Member/Officer Protocol	0	0	0	0	0	0		0
Follow up action relating to breaches of the Member/Officer Protocol	0	0	0	0	0	0		0

Modern Slavery – It is the statutory duty of the Council to refer all concerns raised regarding modern day slavery to the national agencies. This does not mean that Modern Slavery has been confirmed. The case referred in Q1 was found not to be Modern Slavery. The figures show that where reported to the Council, we are promptly complying with our duty to report.

Freedom of Information Requests

	Q1		Q2		Q3		Q4	
	18/19	19/20	18/19	19/20	18/19	19/20	18/19	19/20
Total Number (FOIs)	43	84	57	100	69	79	109	79
% answered on time	84%	99%	96%	95.8%	100%	99%	91%	95.8%
Average per month	14	28	19	33	23	26	36	26
Average response time (days)	12	11	9	10	11	10	10	11
Business as usual (BAUs)	58	59	86	73	55	62	73	65
Transfers (TFRs)	29	18	32	22	32	30	42	33
Subject access requests (SARs)	3	2	3	12	2	6	7	5
Non-compliant requests	0	0	2	0	0	0	0	n/a
Appeals	0	0	0	0	0	0	0	n/a
Withheld due to exemption/fees	7	6	11	18	5	7	10	8
Environmental Information Requests - Land Charges Searches (personal)	40	437	47	367	5	308		334

- Number of FOIs received was steady, inclusive of BAU requests.
- Average response time remained consistent, though slightly longer at 11 days compared to 10 in 19/20 Q3.
- Exemptions for FOIs remained low, while exemptions under BAU more than halved to 8 (not shown here).
- The percentage of requested answered on time has dropped, possibly due to shifting priorities in March to tackle the COVID-19 pandemic.
- During the pandemic, FOI and DPA rules remain the same, however the ICO has stated that it will not penalise public bodies for exceeding time limits where it prioritises COVID-19 related work.

Definitions

Business as usual Information requested can be sent quickly and easily within the normal course of business

Land Charges specific information about a particular property

Ombudsman Complaint a customer has followed Stage 1 and 2 complaints procedure but unhappy with the outcome they are entitled to take complaint to the Local government Ombudsman who will decide if the Council has a case to answer.

Subject Access Request a request by an individual to see information an organisation holds on them

Transfers requests received that fall out of our remit i.e. Adult social Care or Highways

Environmental Information Request a right for any person to request access to environmental information held by public authorities.

This page is intentionally left blank

NORTH WEST LEICESTERSHIRE DISTRICT COUNCIL

AUDIT AND GOVERNANCE COMMITTEE – WEDNESDAY,
22 JULY 2020



Title of Report	STANDARDS AND ETHICS – QUARTER 1 REPORT	
Presented by	Elizabeth Warhurst Head of Legal and Commercial Services	
Background Papers	None	Public Report: Yes
Purpose of Report	To receive the figures for local determination of complaints and the ethical indicators for Quarter 1 of 2020/2021	
Recommendations	THE REPORT BE RECEIVED AND NOTED.	

1. BACKGROUND

- 1.1 The Standards and Ethics Report provides quarterly information in two categories: Local Determination of Complaints and Ethical Indicators. As we enter a new financial year of reporting, those who work together to compile the statistics within it have met and reviewed its format.
- 1.2 Four amendments to the data contained within the report have been made:
- a) Freedom of Information Requests Data within the table at page 4 has been provided in 3 columns per quarter. This is to enable a rolling comparison year on year. To remove the column 18/19 would mean that a comparison could not be made until Q4 when the table was fully populated.
 - b) The row 'Withheld due to exemptions/fees' has been moved up within the table so that it sits directly below Freedom of information Requests and Business as usual. This will give better context as to the amount of exemptions applied to requests.
 - c) The row Appeal has been deleted and replaced with Internal Reviews. This was due to appeals consistently being reported as zero when in fact a number of internal reviews had been requested during 2019/2020.
 - d) The row Regulation of Investigatory Powers Act Indicators has been added to the Ethical Indicators table. This is something that had been reported on until 2018/19 but was taken out following last years review due to the figures consistently being zero. Following an inspection earlier this year we have been advised to include this table in our report.

A definition of RIPA has been added to the definitions page.

Policies and other considerations, as appropriate

Council Priorities:	- Our communities are safe, healthy and connected
Policy Considerations:	N/A
Safeguarding:	Safeguarding in relation to Modern Slavery
Equalities/Diversity:	N/A
Customer Impact:	Customers have the opportunity to report on measures that are included in this report.
Economic and Social Impact:	Detail any economic or social impact as a result of the decision.
Environment and Climate Change:	N/A
Consultation/Community Engagement:	Customers have the opportunity to report on measures that are included in this report
Risks:	By receiving this information members will be able to manage risks.
Officer Contact	Elizabeth Warhurst Head of Legal and Commercial Services elizabeth.warhurst@nwleicestershire.gov.uk

Standards and Ethics

Quarter 1 Report

2020-2021

Contents

Page 1 - Introduction

Page 2 - Local Determinations of Complaints

Page 3 - Ethical Indicators

Page 4 - Freedom of Information Requests

Page 5 - Definitions

Introduction

This is the quarterly report to the Audit & Governance Committee detailing both the figures for the Ethical Indicators and the figures for the Local Determination of Complaints process for 2020/21.

For clarification purposes the months covered by the quarters are as follows:

Quarter 1 - 1 April to 30 June

Quarter 2 - 1 July to 30 September

Quarter 3 - 1 October to 31 December

Quarter 4 - 1 January to 31 March

The report is split into 2 parts for ease of reference; Part 1 refers to the local determination of complaints, part 2 is the table showing the ethical indicators figures.

The report will enable the Audit & Governance Committee to build up a picture over time of how many complaints are received and where these are coming from. The parts of the Code of Conduct which have been breached will also be recorded to enable training to be targeted effectively.

Local Determination of Complaints

The Monitoring Officer received 5 complaints in Quarter 1 of 2020/21.

Of the 5 complaints received, 2 were unable to be progressed as it was determined that the members were not acting in their capacity as councillors and the Code of Conduct was not therefore engaged.

2.1 Assessment Sub-committee Decisions

There has been no Assessment Sub-committee meetings in this quarter.

The Monitoring Officer pursues an informal dispute resolution process prior to initiating formal proceedings via the Sub-committee route.

No complaints have been resolved informally in Quarter 1.

One complaint has been withdrawn in Quarter 1.

2.2 Timeliness of Decision

The Standards for England Guidance stated that the Assessment Sub-committee should complete its initial assessment of an allegation “within an average of 20 working days” to reach a decision on what should happen with the complaint. The Council has taken this standard and adapted it under the new rules to aim to hold an Assessment Sub-committee within 20 working days of notifying the parties that informal resolution is not possible.

2.3 Review Requests

There have been no review requests in Quarter 1. Review requests can only be made following a decision of ‘No further Action’ by the Assessment Sub-committee where there is submission of new evidence or information by the complainant.

2.4 Subsequent Referrals

None to report – see above.

2.5 Outcome of Investigations

There were no investigations concluded in this period.

2.6 Parts of the Code Breached

This section is intended to show where there are patterns forming to enable the Audit and Governance Committee to determine where there needs to be further training for Councillors. Targeting training in this way makes it more sustainable and, hopefully, more effective.

So far this year, the following areas of the code were found to have been breached:

Ethical Indicators

PERFORMANCE INDICATOR ⁰	Q1			Q2			Q3			Q4		
	18/19	19/20	20/21	18/19	19/20	20/21	18/19	19/20	20/21	18/19	19/20	20/21
Instances of concerns raised re Modern Slavery	n/a	0	0	n/a	1		n/a	0		n/a	0	
Instances of concerns raised re Modern Slavery referred to national agencies	n/a	1	0	n/a	1		n/a	0			0	
Number of whistle blowing incidents reported	0	0	0	0	0		0	0		n/a	0	
Number of Challenges to procurements	n/a	0	0	n/a	0		n/a	0			0	
Public interest Reports	0	0	0	0	0		0	0			0	
Objections to the Councils Accounts	0	0	0	0	0		0	0			0	
Disciplinary action relating to breaches of the Member/Officer Protocol	0	0	0	0	0		0	0			0	
Follow up action relating to breaches of the Member/Officer Protocol	0	0	0	0	0		0	0		n/a	0	
Use of RIPA powers*	0	0	0	0	0		0	0		0	0	

*this was an ethical indicator previously reported on until 2019. It was not reported on during 19/20 but a recent RIPA inspection has recommended the reintroduction of reporting on this indicator. Internal Audit have however been able to provide retrospective data to cover 19/20.

Freedom of Information Requests

	Q1			Q2			Q3			Q4		
	18/19	19/20	20/21	18/19	19/20	20/21	18/19	19/20	20/21	18/19	19/20	20/21
Total Number (FOIs)	43	84	55	57	100		69	79		109	79	
% answered on time	84%	99%	72.2%	96%	95.8%		100%	99%		91%	95.8%	
Average per month	14	28	18	19	33		23	26		36	26	
Average response time (days)	12	11	15	9	10		11	10		10	11	
Business as usual (BAUs)	58	59	27	86	73		55	62		73	65	
Withheld due to exemption/fees (BAU & FOI)*	7	6	10	11	18		5	7		10	8	
Transfers (TFRs)	29	18	14	32	22		32	30		42	33	
Subject access requests (SARs)	3	2	3	3	12		2	6		7	5	
Internal Reviews**	tbc	tbc	1	tbc	tbc		tbc	tbc		tbc	2	
Environmental Information Requests/ Land Charges Searches (personal)	40	437	213	47	367		5	308			334	

* Withheld due to exemptions has been moved up the table so that it sits below FOI's and BAU's thereby making it easier to compare and put into context the number of exemptions applied.

** Appeals has been amended to Internal Review as appeals were consistently zero but a number of reviews had been requested during 2019/2020.

All statistics presented from 19/20 Q4 should be viewed in the context of the pandemic and the subsequent disruption to services. FOI timescale for response is 20 days, however the ICO has expressed leniency given that work relating to the pandemic should be given priority over completing FOI work.

- Q1 has seen a **drastic reduction** in the total number of **FOIs and BAUs received, 82**. This is the lowest result on record.
Compare to:
 - 19/20 average of 150 p/Q and;
 - Q1 average of 125 p/Q.
- **Average response time** has risen to a record high of **15 days**.
- **% answered on time** has dropped to a record low of **72.2%** in the same manner.
- The number of **TFRs, SARs, and EIR/Land Charge Searches** received have dropped similarly to FOIs and BAUs.
- Past data regarding **Internal Reviews** is being collated.

Definitions

Business as usual Information requested can be sent quickly and easily within the normal course of business

Land Charges specific information about a particular property

Ombudsman Complaint a customer has followed Stage 1 and 2 complaints procedure but unhappy with the outcome they are entitled to take complaint to the Local government Ombudsman who will decide if the Council has a case to answer.

Subject Access Request a request by an individual to see information an organisation holds on them

Transfers requests received that fall out of our remit i.e. Adult social Care or Highways

Environmental Information Request a right for any person to request access to environmental information held by public authorities.

RIPA The Regulation of Investigatory Powers Act 2000 regulates public bodies ability to carry out surveillance, investigation and the interception of communications.

This page is intentionally left blank

Title of Report	DRAFT MEMBER CONDUCT ANNUAL REPORT	
Presented by	Elizabeth Warhurst Head of Legal & Commercial Services and Monitoring Officer	
Background Papers	Localism Act 2011 http://www.legislation.gov.uk/ukpga/2011/20/contents/enacted Current NWL Code of Conduct Available on the Council's website and in the Constitution www.nwleics.gov.uk	Public Report: Yes
Purpose of Report	To receive and note the draft Annual Report and authorise the Head of Legal & Commercial Services and Monitoring Officer to make any minor amendments before being recommended to Council.	
Recommendations	(1) THAT THE DRAFT MEMBER CONDUCT ANNUAL REPORT 2019/20 BE RECEIVED AND NOTED; (2) THAT AUTHORITY BE DELEGATED TO THE HEAD OF LEGAL AND COMMERCIAL SERVICES AND MONITORING OFFICER TO MAKE ANY MINOR AMENDMENTS TO THE REPORT FOLLOWING COMMENTS FROM THE AUDIT AND GOVERNANCE COMMITTEE; (3) THAT COUNCIL BE RECOMMENDED TO ENDORSE THE MEMBER CONDUCT ANNUAL REPORT 2019/20.	

1.0 INTRODUCTION

- 1.1 It is important that the work of the Audit and Governance Committee should be visible to the Authority and wider public. It is felt that the annual report acts as a helpful tool in communicating the work undertaken by the Audit and Governance Committee to the public and to Members.
- 1.2 The Committee is recommended to receive and note the draft Member Conduct Annual Report 2019/20 and authorise the Head of Legal and Commercial Services and Monitoring Officer to make any necessary amendments following comments from this Committee before being recommended to Council for endorsement.

Policies and other considerations, as appropriate	
Council Priorities:	Supporting Coalville to be a more vibrant, family-friendly town Support for businesses and helping people into local jobs Developing a clean and green district Local people live in high quality, affordable homes Our communities are safe, healthy and connected
Policy Considerations:	Code of Conduct and Constitution
Safeguarding:	N/A
Equalities/Diversity:	Detailed in the Annual Report attached as an appendix.
Customer Impact:	N/A
Economic and Social Impact:	N/A
Environment and Climate Change:	N/A
Consultation/Community Engagement:	N/A
Risks:	By receiving this information members will be able to manage risks of misconduct.
Officer Contact	Elizabeth Warhurst Head of Legal & Commercial Services and Monitoring Officer elizabeth.warhurst@nwleicestershire.gov.uk



MEMBER CONDUCT ANNUAL REPORT 2019-20

1. Introduction

This is the Member Conduct Annual Report of North West Leicestershire District Council's Audit and Governance Committee and covers the period from 1 April 2019 to 31 March 2020.

In addition to the responsibilities detailed in the Terms of Reference below, the Audit and Governance Committee promotes high standards of conduct by District Council Members and Members of Town / Parish Councils in North West Leicestershire. The Audit and Governance Committee complies with the requirements of the Localism Act 2011, the Regulations and the guidance provided under that legislation, together with Council's adopted Arrangements.

On 27 June 2012 Council adopted the North West Leicestershire Code of Conduct for Members which had been drafted by Members for Members. The Code incorporates all the legislative requirements under the Localism Act 2011 in relation to Disclosable Pecuniary Interests together with retaining the personal obligations in existence under the previous regime.

2. Audit and Governance Committee Terms of Reference

Membership: Ten District Councillors

Quorum: Three District Councillors

Terms of Reference during the 2019-2020 financial year:

Statement of purpose

1. The Audit & Governance Committee is a key component of North West Leicestershire District Council's corporate governance. It provides an independent and high-level focus on the audit, assurance and reporting arrangements that underpin good governance and financial standards.
2. The purpose of the Audit & Governance Committee is to provide independent assurance to those charged with governance of the adequacy of the risk management framework and the internal control environment. It provides independent review of North West Leicestershire District Council's governance, risk management and control frameworks and oversees the financial reporting and annual governance processes. It oversees internal audit and external audit arrangements, helping to ensure efficient and effective assurance mechanisms are in place.

Governance, risk and control

3. To review the council's corporate governance arrangements against the good governance framework, including the ethical framework and consider the local code of governance.
4. To review the Annual Governance Statement prior to approval and consider whether it properly reflects the risk environment and supporting assurances, taking into account internal audit's opinion on the overall adequacy and effectiveness of the council's framework of governance, risk management and control.
5. To consider the council's arrangements to secure value for money and review assurances and assessments on the effectiveness of these arrangements.
6. To consider the council's framework of assurance and ensure that it adequately addresses the risks and priorities of the council.
7. To monitor and provide scrutiny over the effective development and operation of risk management in the council.

8. To monitor progress in addressing risk-related issues reported to the committee such as the Corporate Risk Register.
9. To consider reports on the effectiveness of internal controls and monitor the implementation of agreed actions.
10. To review the assessment of fraud risks and potential harm to the council from fraud and corruption.
11. To monitor the Anti-Fraud and Corruption strategy, actions and resources.

Internal audit

12. To approve the internal audit charter.
13. To approve (but not direct) the risk-based internal audit plan, including internal audit's resource requirements, the approach to using other sources of assurance and any work required to place reliance upon those other sources.
14. To approve significant interim changes to the risk-based internal audit plan and resource requirements.
15. To make appropriate enquiries of both management and the head of internal audit to determine if there are any inappropriate scope or resource limitations.
16. To consider any impairments to independence or objectivity arising from additional roles or responsibilities outside of internal auditing of the head of internal audit. To approve and periodically review safeguards to limit such impairments.
17. To consider progress reports from the head of internal audit on internal audit's performance during the year
18. To consider the head of internal audit's annual report, including the statement of the level of conformance with the Public Sector Internal Audit Standards and the results of the Quality Assurance and Improvement Programme that supports the statement. Fundamental to the annual report is the opinion on the overall adequacy and effectiveness of the council's framework of governance, risk management and control together with the summary of the work supporting the opinion. These will assist the committee in reviewing the Annual Governance Statement.
19. To consider summaries of specific internal audit reports in accordance with agreed protocols.
20. To receive reports outlining the action taken where the head of internal audit has concluded that management has accepted a level of risk that may be unacceptable to the authority or there are concerns about progress with the implementation of agreed actions.
21. To contribute to the QAIP and in particular, to the external quality assessment of internal audit that takes place at least once every five years.
22. To provide free and unfettered access to the audit committee chair for the head of internal audit, including the opportunity for a private meeting with the committee.

External audit

23. To support the independence of external audit through consideration of the external auditor's annual assessment of its independence and review of any issues raised.

24. To consider the external auditor's annual letter, relevant reports and the report to those charged with governance.
25. To consider specific reports as agreed with the external auditor.
26. To comment on the scope and depth of external audit work and to ensure it gives value for money.

Financial reporting

27. To review the annual statement of accounts. Specifically, to consider whether appropriate accounting policies have been followed and whether there are concerns arising from the financial statements or from the audit that need to be brought to the attention of the council.
28. To consider the external auditor's report to those charged with governance on issues arising from the audit of the accounts.
29. To seek assurances that the council has complied with the Treasury Management Strategy and Practices by demonstrating effective control of the associated risks and pursuing optimum performance consistent with those risks.

Accountability arrangements

30. To report to those charged with governance on the committee's findings, conclusions and recommendations concerning the adequacy and effectiveness of their governance, risk management and internal control frameworks, financial reporting arrangements, and internal and external audit functions.
31. To report to full council on a regular basis on the committee's performance in relation to the terms of reference and the effectiveness of the committee in meeting its purpose.
32. To publish an annual report on the work of the committee.

Functions	Matters reserved for a Decision
The Council has determined under the powers conferred on it by Section 28(6) of the Localism Act 2011 to appoint an Audit and Governance Committee and it has the following roles and functions:	To determine any issues referred to the Committee (except for any matter reserved to the Council).
Promoting and maintaining high standards of conduct by councillors and co-optees Assisting the councillors and co-optees to observe the Members' Code of Conduct Advising the Council on the adoption or revision of the Members' Code of Conduct Monitoring the operation of the Members' Code of Conduct Advising, training or arranging to train councillors and co-opted members on matters relating to the Members' Code of Conduct Granting dispensations to councillors who require such dispensations for more than	

<p>one meeting or on more than one occasion from requirements relating to interests set out in the Members Code of Conduct as appropriate</p> <p>Dealing with any report from the Monitoring Officer on any matter concerning Governance</p> <p>To establish Sub-committees for the Assessment of Determination of matters concerning allegations of Members Conduct</p> <p>And in addition the Audit and Governance Committee also oversees the ethical framework of the Council including oversight of:</p> <ul style="list-style-type: none"> • the Whistle Blowing Policy • complaints handling • Ombudsman investigations 	
To exercise the above functions for the parish councils wholly or mainly in its area and the members of those parish councils.	

Sub-committees of the Audit and Governance Committee

All Audit and Governance Committee members will form a pool from which members will be drawn based on their availability and the requirements of the particular Sub-committee as and when required.

Assessment Sub-committee

Assessment of complaints in accordance with the Council's Guidance and to either:

- Accept the Monitoring Officer's recommendation of no failure to comply with the Code of Conduct
- Refer the matter for full investigation
- Refer the matter for other action

Review Sub-committee

Consideration of requests for a review in accordance with the Council's Guidance.

Determinations Sub-committee

To receive reports from the Monitoring Officer or her appointed investigating officer and to decide either:

- To determine finding of no failure to comply with the Code of Conduct
- To determine finding of failure to comply with the Code of Conduct and impose relevant sanctions
- Refer the matter for other action

in accordance with the Council Guidance

3. Composition

District Councillors

All appointed by Council on 21 May 2019

Chairman: Councillor V Richichi

Deputy Chairman: Councillor D Harrison

Councillor C Benfield

Councillor D Bigby

Councillor J Clarke

Councillor L Gillard

Councillor S Gillard

Councillor M Hay

Councillor S Sheahan

Councillor M Wyatt

Parish Representatives

Following the District and Parish elections in May 2019 nominations for Parish Representatives have been sought from all Town and Parish Councils to fill the four seats. Seven nominations were received and a ballot is currently being held to select the representatives. The ballot closes on Friday, 13 March 2020 and the count will be held prior to the next meeting.

Independent Persons

The legislation requires the Council to appoint at least one Independent person who potentially advises all those involved in a Standards complaint, including the Monitoring Officer, and who must be consulted prior to the determination of a complaint.

Through an open advertising process conducted with partner authorities the Council appointed the following pool of independent persons from whom one can be drawn as and when required:

Michael Pearson

Mark Shaw

Christine Howell

Gordon Grimes

Richard Gough

The main officer support for the Committee is provided by the Monitoring Officer (Elizabeth Warhurst), the Deputy Monitoring Officer (Elisabeth Tomlinson) and the Democratic Support Officer (Rachel Wallace).

4. Meetings and Work Programme

The Audit and Governance Committee meets a minimum of four times per annum. In addition to its scheduled meetings, sub committees still meet on an ad hoc basis in order to consider and determine allegations of Member conduct. The Committee has its main work planned in advance through a Work Programme which enables it to be more proactive, strategic and focused in its approach to key issues.

5. Reporting Arrangements

The Audit and Governance Committee receives quarterly reports which have enabled Members to be reminded of the issues it has dealt with during each quarter and address any issues which this has highlighted.

6. Procedures and Workloads

(a) Dispensations

During 2018/19, there were no applications received for a dispensation from either District or Parish members.

(b) Complaints made to the Monitoring Officer under the Code of Conduct during 2019/20

Complaints made: 1

by Members of the Public	0
by Parish Councillors	0
by District Councillors	1
by Parish Clerk	0
by Council Officer	0

Complaints against:

a Parish Councillor	0
a District Councillor	1

From the above mentioned complaints:

1 complaint was resolved informally:

This complaint related to unprofessional conduct of a councillor.

0 complaints were withdrawn:

0 complaints are at informal resolution stage:

(c) Complaints referred to the Standards Assessment Sub Committee

From the above-mentioned complaints: - None

(d) Members' Register of Interests

The Democratic Services Officers undertake regular checks of the Register of Members' Interests and provide advice and assistance to Parish Councils on the completion of the Registers.

(e) Advice and Training

The Monitoring Officer and Deputy Monitoring Officer continue to provide both parish and district members with advice, both proactively and on request, on member's interests and all aspects of corporate governance.

Following the District and Parish Council Elections in May 2019, training on the Code of Conduct was offered to all District and Parish Members.

Training is also currently being provided to members on all aspects of data protection and freedom of information.

7. Policies & Procedures

The Audit and Governance Committee oversees the ethical framework of the Council including oversight of:

- the Whistle Blowing Policy

- complaints handling
- Ombudsman investigations.
- Freedom of Information and Data Protection

**Elizabeth Warhurst
Monitoring Officer**

**Councillor V Richichi
Chairman**

OUR VISION




North West Leicestershire will be a place where people and businesses feel they belong and are proud to call home

**Legal and Support Services
North West Leicestershire District Council**

NORTH WEST LEICESTERSHIRE DISTRICT COUNCIL

AUDIT AND GOVERNANCE COMMITTEE – WEDNESDAY
22 JULY 2020



Title of Report	REVIEW OF MODEL MEMBER CODE OF CONDUCT	
Presented by	Elizabeth Warhurst Head of Legal & Commercial Services and Monitoring Officer	
Background Papers	<p>Report to Council – 26 June 2012 - Localism Act 2011 Standards Regime</p> <p>Report to Council – 11 November 2014</p> <p>Localism Act 2011: http://www.legislation.gov.uk/ukpga/2011/20/contents/enacted</p> <p>Current NWLDC Code of Conduct – Available on the Council's website and in the Constitution www.nwleics.gov.uk</p> <p>Consultation Draft LGA Model Member Code of Conduct: 2020320-lga-consultation-draft-model-member-code-of-conduct-update-27-march-2020 - Shortcut.Ink</p> <p> 2020.3.20 LGA Consultation Draft 1</p> <p> 2020.3.20 Appendices A-B LGA</p> <p> pdf version code of conduct consultatio</p> <p>Standards in Public Life report published on 30th January 2019: https://www.gov.uk/government/publications/local-government-ethical-standards-report</p>	Public Report : Yes
Purpose of Report	To seek feedback on the Consultation Draft LGA Model Member Code of Conduct	
Recommendation	THAT THE CONSULTATION DRAFT LGA MEMBER MODEL CODE OF CONDUCT 2020 AND QUESTIONNAIRE BE CONSIDERED AND FEEDBACK PROVIDED TO THE LGA	

1. INTRODUCTION

- 1.1 On the 17 June 2020, Members were asked to submit feedback on the draft LGA Member Code of Conduct 2020 and questionnaire by the 8 July 2020. As at the date of writing this report no substantive feedback has been received. However, any feedback provided by members will be circulated to the Committee prior to the meeting.

2. BACKGROUND

- 2.1 The Localism Act 2011 (“the Act”) made fundamental changes to the system of regulating standards of conduct for elected and co-opted Members making each Authority responsible for its own Members. The duty now lies with the individual Authorities (and their Monitoring Officer) to investigate and hold to account Members accused of breaches. These changes were enacted on 1 July 2012.
- 2.2 Section 27 (1) of the Act requires a local authority to promote and maintain high standards of conduct by its members and co-opted members. In discharging its duty, pursuant to Section 27 (2) of the Act an authority must adopt its own local Member Code of Conduct setting out the behaviours and responsibilities expected of members and co-opted members in their roles.
- 2.3 At its meeting on the 26th June 2012, the Council resolved to formally adopt its own local member model code of conduct suitably drafted to reflect the changes brought about by the Act. The code was further updated in November 2014 and since then no further changes have been made. The current version of the code contained within the NWLDC Constitution is attached to this report.

3. DRAFT MEMBER CODE OF CONDUCT CONSULTATION

- 3.1 A CoPSL report was published on 30 January 2019 which recommended that “*The Local Government Association should create an updated model code of conduct, in consultation with representative bodies of Councillors and officers of all tiers of local government in consultation with representatives following the recommendations of the Committee of Standards in Public Life report published on 30 January 2019*”.
- 3.2 The Board of the LGA at its meeting on 11 September 2019 considered and agreed to commence reviewing of the Code ahead of central government’s response to the recommendations of the report. This has been done in response to recommendations made by the Committee on standards in Public Life, and also in response to rising local government concern about increasing incidence of public, member-to-member and officer/member intimidation and abuse and overall behavioural standards and expectations in public debate, decision making and engagement.
- 3.3 If the draft model code is completed before any government response to the CoPSL report, Local Authorities will be able to adopt the Code. Some of the recommendations in the CoPSL report for example the power to suspend councillors (recommendation 16 of the CoPSL report on, page 16) , requires legislation which means that provisions cannot be included in the Code.
- 3.4 The LGA aims to develop a code that benchmarks a standard for all public office and for those engaged in public discourse and debate. This includes producing a code that is fit for purpose, useful and held in high regard, articulate what local government believes are good standards for all in public office and to enhance the reputation of local government and local politicians.

- 3.5. The adoption of the draft model code is not mandatory. There is no legislative requirement for this authority to adopt the draft model code and it may continue to rely on the current version. However, the draft model code has been provided by the LGA as part of its work on supporting the sector to continue to aspire to high standards of leadership and performance and as a member authority and stakeholder we have been asked to provide feedback and comments. This draft model code is offered as a template for Council's to adopt in whole and/or with local amendment and should be able to be adapted by individual authorities.
- 3.6 It is considered that a model code would create consistency across England, and reflect the common expectations of the public regardless of geography or tier. It would also reduce the potential for confusion among dual-hatted or triple-hatted councillors. Areas such as gifts and hospitality, social media use, and bullying and harassment have all increased in salience, and are not regularly reflected in local authority codes of conduct. All local authorities need to take account of these areas, and a model code of conduct would help to ensure that they do so.

4 NEXT STEPS

- 4.1 The consultation on the draft member code of conduct will run for 10 weeks from **Monday 8 June** until **Monday 17 August**. It is hoped that this will provide officers and members with enough time to reflect on the draft model member code of conduct and questionnaire and provide the LGA with feedback. The feedback from the consultation will help them develop a final draft, which will be reviewed by the LGA's Executive Advisory Board before being presented to the next LGA General Assembly, which it is hoped will be held in the Autumn of 2020.
- 4.2 Members are requested to consider the contents of the draft LGA model code of conduct attached with a view to providing a joint response to the questionnaire at this meeting. Once the authority has provided its feedback to the LGA, The LGA will provide formal consultation questions and then take on board the comments and direction and put forward a final code for formal adoption at the LGA General Assembly later this year.

Policies and other considerations, as appropriate	
Council Priorities:	Insert relevant Council Priorities: <ul style="list-style-type: none"> - Supporting Coalville to be a more vibrant, family-friendly town - Support for businesses and helping people into local jobs - Developing a clean and green district - Local people live in high quality, affordable homes - Our communities are safe, healthy and connected
Policy Considerations:	Code of Conduct and Constitution
Safeguarding:	N/A
Equalities/Diversity:	N/A
Economic and Social Impact:	N/A
Environment and Climate Change:	N/A
Consultation/Community Engagement:	All District Councillors
Risks:	This report is for consideration and feedback to the LGA and by receiving this draft code of conduct members will be able to consider and manage risks of misconduct
Officer Contact	Elizabeth Warhurst Head of Legal and Commercial Services elizabeth.warhurst@nwleicestershire.gov.uk

NORTH WEST LEICESTERSHIRE DISTRICT COUNCIL

AUDIT AND GOVERNANCE COMMITTEE – WEDNESDAY,
22 JULY 2020



Title of Report	UPDATE OF THE COUNCIL'S CONSTITUTION	
Presented by	Elizabeth Warhurst Head of Legal and Commercial Services and Monitoring Officer	
Background Papers	Council Procedure Rules Contract Procedure Rules	Public Report: Yes
Purpose of Report	To seek comments and recommendations to Council on proposed amendments arising from the Annual Review of the Constitution.	
Recommendations	<p>1. THAT THE AMENDMENTS TO THE COUNCIL'S CONSTITUTION SET OUT IN THIS REPORT ARE ADOPTED.</p> <p>2. THAT COUNCIL AUTHORISES THE HEAD OF LEGAL AND COMMERCIAL SERVICES TO MAKE THE AGREED AMENDMENTS AND ANY CONSEQUENTIAL AMENDMENTS TO THE CONSTITUTION AND RE-ISSUE THE DOCUMENT.</p>	

1. INTRODUCTION

- 1.1 The Local Government Act 2000 requires each Local Authority to prepare, keep up to date and publicise the document known as the Constitution.
- 1.2 The Constitution should be logical, integrated and accessible to Members, officers, local people and anyone else interested in the way a local authority makes its decisions. There is also a statutory requirement on the Council's Monitoring Officer to keep the Constitution up to date, and accordingly the update of the Constitution is an on-going process. The Monitoring Officer has delegated powers to make any necessary changes to the Constitution to reflect changes of fact and law, and decisions of the Council and of the Cabinet.
- 1.3 Full Council regularly considers items relating to updates to the Constitution. The updates are generally required due to legislative and organisational changes or to clarify and improve processes within the Authority to reflect best practice.
- 1.4 In parallel with this process the Legal Services Team reviews any proposed legislation which is likely to require amendments to the Constitution.

- 1.5 Relevant Managers within the Authority have been consulted as to whether they require any changes to be made to the Constitution in relation to their service areas and although this has yielded very few requests, those that have been requested are reflected within this report.

2. PROPOSED CHANGES

Proposed Changes to the Constitution are detailed below:

2.1 Change to Part 4, 4.7 Contract Procedure Rule 1.4 (c)

NWLDC's Standing Orders, contained within the Constitution, are made pursuant to S.135 of the Local Government Act 1972. They have been prepared in accordance with the Public Contracts Regulations 2015, the Authority's policies and to facilitate small and medium enterprises in the local area the opportunity to enter into the Authority's supply chain.

The Standing Orders contained in Part 4 (4.7) of the Constitution (the Contract Procedure Rules) set out how the Authority will invite tenders, obtain quotations and award contracts for supplies, services or works. Financial Procedures provide the framework for managing the Council's financial affairs. They are supported by more detailed Financial Management Standards which set out how the procedures will be implemented.

Where the Authority is disposing of goods, officers are required to seek advice from the Head of Finance and have regard to the provisions of the Financial Procedure Rules.

These rules do not apply to:

- (a) contracts with local authorities for the joint delivery of services or discharge of functions, save the obligation to secure value for money for the Authority;
- (b) transactions for the sale, purchase or lease of land or property;
- (c) Contracts which benefit from any exemption to the Public Contracts Regulations 2015 contained in Regulation 12 of those regulations.

It is proposed to widen CPR 1.4 (c) above to include reference to Regulation 10 of the PCR 2015. This will allow us to award service contracts specifically excluded from the Public Contracts Regulations 2015. As currently drafted our Contract Procedure Rules would require us to undertake a competitive tender where this is not required by the Regulations. The inclusion of Regulation 10 at CPR 1.4 (c) does not prohibit us from undertaking a competitive tender should we so wish in order to ensure value for money, it simply removes the necessity to complete one where not practical or appropriate.

The Contract Procedure Rules are appended to this report. The amended Rule 1.4. © is set out below with tracked change indicated in red:

“ 1.4. (C) contracts which benefit from any exemption to the Public Contracts Regulations 2015 contained in Regulation 10 and/or 12 of those regulations”

“contracts which benefit from any exemption to the Public Contracts Regulations 2015 contained in Regulation 10 and/or 12 of those regulations

2.2 Change to Part 4, 4.1 Council Procedure Rules 4.3

The Council Procedure Rules (CPR's) are set out in Part 4 of the Constitution and constitute the Council's statutory procedural standing orders which apply to running of Council meetings. By virtue of Rule 4.2. Rule 4.2 applies many of these CPR's to the Authority's Boards and Committees. CPR 10 which relates to questions raised by the public at Cabinet and ordinary meetings of the Council, and which is set out in the appendix to this report, does not apply specifically to Boards and Committees. However, by virtue of Rule 4.3, CPR 10 has been specifically applied to Scrutiny Committee.

Although the Terms of Reference of the Local Plan Committee refer to questions made by the Public at its meetings, there is no specific application of CPR 10 by virtue of Rule 4.3 and for clarity and consistency purposes, it is now proposed to reference the application of CPR 10 to the Local Plan Committee by virtue of Rule 4.3. The proposed amended Rule 4.3 is set out below with tracked change indicated in red:

"4.3. Rule 10 – questions by the public shall apply to Scrutiny Committees and Local Plan Committee."

2.3 Addition to Council Procedure Rules - Remote Meeting Procedure Rules (Temporary Standing Order 4A)

- 2.3.1 During the current Covid 19 pandemic, everyone is experiencing a fast paced period of change and uncertainty. Indeed, following the closure of the Council Offices, and requirements to limit social interaction and safeguard those in vulnerable health groups, it has been necessary to change the way meetings are held to enable remote access.
- 2.3.2 Remote meetings of the Council, and its various Committees and Sub-committees have been successfully held remotely since April 2020. To regularise the position It is therefore requested that a suitable set of Rules around remote meeting procedures be added to the existing Council Procedure Rules whilst the relevant Regulations referred to below remain in force. These additional Rules will be referred to as "The Remote Meetings Procedure Rules" and are attached by way of an appendix to this report. All available legal and senior officers have been consulted.
- 2.3.3 "The Remote Meetings Procedure Rules" are required to be incorporated into the Constitution for the purpose(s) of giving operational effect to the provision(s) as contained under Section 78 of the Coronavirus Act 2020 ("the 2020 Act") and the Local Authorities and Police and Crime Panels (Coronavirus) (Flexibility of Local Authority and Police and Crime Panel Meetings) (England and Wales) Regulations 2020 ("the 2020 Regulations")
- 2.3.4 The purpose of the Remote Meetings Procedure Rules is to provide the means and guidance for the conduct of any remote meeting of the Council, its various Committees and Sub-committees, held under the provisions of the 2020 Regulations and should be read in conjunction with the Council Procedure Rules under Part 4 of the Constitution. The 2020 Regulations made under Section 78 of the 2020 Act apply notwithstanding any other legislation or current or pre-existing standing orders or any other procedure rules of the Council governing meetings and remain valid until 7 May 2021. Legislation will be required to

extend these Regulations. In the event of any conflict, the Remote Meetings Procedure Rules take precedence in relation to any remote meetings.

3. FUTURE REVIEWS

- 3.1 Work is currently underway to prepare Social Media Guidance for Members that will tie into the Code of Conduct so that there is clarity over what constitutes actions carried out “in the capacity of a Member”. In addition to this, the LGA are currently undertaking a review of the Model Member Code of Conduct and any changes to the Constitution as a result of this will be brought to the Council in due course.

Policies and other considerations, as appropriate	
Council Priorities:	Relevant Council Priorities: <ul style="list-style-type: none"> - Supporting Coalville to be a more vibrant, family-friendly town - Support for businesses and helping people into local jobs - Developing a clean and green district - Local people live in high quality, affordable homes - Our communities are safe, healthy and connected
Policy Considerations:	N/A.
Safeguarding:	N/A
Equalities/Diversity:	N/A
Customer Impact:	N/A
Economic and Social Impact:	N/A
Environment and Climate Change:	N/A
Consultation/Community 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. None Identified.
Officer Contact	Elizabeth Warhurst Head of Legal and Commercial Services and Monitoring Officer 01530 454762 elizabeth.warhurst@nwleicstershire.gov.uk

Standing Order (Temporary) Part 4.1 (A)

REMOTE MEETINGS PROCEDURE RULES

These standing orders provide the rules for the conduct of any meeting which the Council has determined will be suitable for remote conferencing of the Council and its various Committees and Sub-Committees pursuant to The Local Authorities and Police and Crime Panels (Coronavirus)(Flexibility of Local Authority and Police and Crime Panel Meetings)(England and Wales) Regulations 2020.

Members may be able to participate by means of conferencing if so agreed by the Chair of the Meeting in accordance with arrangements agreed from time to time by the Council. Attendance by conferencing will be with the agreement of the Chair and process for arranging attendance as set out in these Procedure Rules must be complied with.

1. How will Notice of Meetings be Provided

- 1.1 The Proper Officer will give notice to the public of the time of the meeting and shall provide details of how the meeting shall be open to the public which shall be through remote means including (but not limited to) video conferencing and live interactive streaming.
- 1.2 Members will be notified of a remote meeting by email and all agenda papers will be available on the Authority's website and via its meeting management software or other electronic means as appropriate. Hard copies of agendas will be sent to those Members who sit on the Committee.

2. Application of the Meetings Procedure Rules

- 2.1 These Procedure Rules should be read in conjunction with the [Council General Procedure Rules](#) which details the rules of debate and apply to all meetings of the Council except as varied by Committee Procedure Rules.

3. Quorum

- 3.1 Any Member so authorised to participate by remote conferencing shall be regarded as present for the purposes of determining a quorum.
- 3.2 In the event of any failure of the video conferencing link the Chair will immediately determine if the meeting is still quorate, if it is then the business of the meeting will continue, if there is no quorum then the meeting will only in such circumstances, adjourn for a period specified by the Chair to allow the connection to be re-established.

4. Notice of Remote Link

- 4.1 Any Member wishing to participate by remote means in any meeting of the Council, or of a Committee or Sub-committee, must confirm their attendance by such means in writing to Democratic Services at least 48 hours in advance of the start of the meeting.
- 4.2 The remote means must be established and tested before the commencement of the meeting.

5. Types of Remote Link

- 5.1 Members should try to establish video conferencing capability however by exception, they may attend by audio only.

6. Record of Attendance

- 6.1 The Chair will confirm at the outset and at any reconvening of the meeting that they can see and hear all participating Members. Any Member participating by remote link must also confirm at the outset and at any reconvening of the meeting that he/she can see and hear the proceedings and the other attendees.
- 6.2 Democratic Services will record attendance on behalf of Members.

7. Declaration of Interests

- 7.1 Any Member participating by remote link who declares an interest in any item of business in terms which requires them to leave the room must also leave the remote conference. The departure will be confirmed by Democratic Services. This member of staff will thereafter confirm to the remote Member when they may re-join the meeting.

8. Disruption to Remote Conferencing

- 8.1 Should any aspect of the conference link fail, the Chair may call a short adjournment of up to five minutes to determine whether the link can quickly be re-established. Efforts should continue to re-establish the link but the meeting shall continue to deal with the business whilst this happens providing the meeting remains quorate.
- 8.2 In the event of link failure, the remote Member(s) will be deemed to have left the meeting at the point of failure of the equipment and if the link cannot be re-established before the end of the meeting then the presumption will be that the meeting should continue to deal with the item. If the link is successfully re-established then the remote Member(s) will be deemed to have returned at the point of re-establishment.

9. Notification of Right to Speak

- 9.1 The Chair shall determine at the commencement of the meeting how Members should notify them that they wish to speak considering whether video or audio conferencing is being used.
- 9.2 Officers of the Council should notify the Chair when they wish to speak in the same way as Members.

10. Voting

- 10.1 A remote Member participating in a vote will cast his/her vote as if participating in a recorded vote. Democratic Services will confirm the vote (for, against, abstentions and whether the motion has been carried or lost) to the Chair.

11. Exclusion of Public

If a remote Member wishes to participate in discussion of a confidential/exempt item they must verify that the venue is secure, that no member of the public has access and that no recording of the proceedings is being made, by any person. The members of staff present will ensure that no recording is taking place.

AUDIT AND GOVERNANCE COMMITTEE – WORK PROGRAMME (as at 14/07/20)

Issue	Report Author	Meeting at which will be reported
October		
Internal Audit Progress Report	Lisa Marron, Audit Manager	21 October 2020
Treasury Management Activity Report	Anna Wright, Finance Team Manager	21 October 2020
Corporate Risk Update	Tracy Bingham, Head of Finance	21 October 2020
Standards & Ethics – Quarterly Report	Elizabeth Warhurst, Head of Legal and Commercial Services	21 October 2020
Report to Those Charged with Governance	Tracy Bingham, Head of Finance	21 October 2020
November (additional meeting)		
Annual Statement of Accounts 2019/20	Tracy Bingham, Head of Finance	24 November 2020
Annual Governance Statement 2019/20	Tracy Bingham, Head of Finance	24 November 2020
January		
Internal Audit Progress Report	Lisa Marron, Audit Manager	20 January 2021
Treasury Management Activity Report	Anna Wright, Finance Team Manager	20 January 2021
Corporate Risk Update	Tracy Bingham, Head of Finance	20 January 2021
Standards & Ethics – Quarterly Report	Elizabeth Warhurst, Head of Legal and Commercial Services	20 January 2021
Annual Audit Letter	Tracy Bingham, Head of Finance	20 January 2021
External Audit Progress Report	Tracy Bingham, Head of Finance	20 January 2021
External Audit Plan	Tracy Bingham, Head of Finance	20 January 2021

Issue	Report Author	Meeting at which will be reported
April		
Internal Audit Progress Report	Lisa Marron, Audit Manager	21 April 2021
Treasury Management Stewardship report 2020/21	Anna Wright, Finance Team Manager	21 April 2021
Corporate Risk Update	Tracy Bingham, Head of Finance	21 April 2021
Standards & Ethics – Quarterly Report	Elizabeth Warhurst, Head of Legal and Commercial Services	21 April 2021
Accounting Policies and Materiality 2020/21	Tracy Bingham, Head of Finance	21 April 2021
Annual Report on Grants and Claims	Tracy Bingham, Head of Finance	21 April 2021
Draft Member Conduct Annual Report	Elizabeth Warhurst, Head of Legal and Commercial Services	21 April 2021