North West Leicestershire District Council

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

Meeting	**CABINET**
Time/Day/Date	5.00 pm on Tuesday, 19 September 2023
Location	Abbey Room, Stenson House, London Road, Coalville, LE67 3FN
Officer to contact	Democratic Services (01530 454512)

AGENDA

Item		Pages
1.	**APOLOGIES FOR ABSENCE**	
2.	**DECLARATION OF INTERESTS** Under the Code of Conduct members are reminded that in declaring interests you should make clear the nature of that interest and whether it is a disclosable pecuniary interest, registerable interest or other interest.	
3.	**PUBLIC QUESTION AND ANSWER SESSION**	
4.	**MINUTES** To confirm the minutes of the meeting held on 22 August 2023	**3 - 4**
5.	**REVIEW OF CORPORATE GOVERNANCE POLICIES** The report of the Strategic Director of Resources	**5 - 166**
6.	**2023/24 QUARTER 1 GENERAL FUND AND HOUSING REVENUE ACCOUNT (HRA) FINANCE UPDATE** The report of the Strategic Director of Resources	**167 - 208**
7.	**MINUTES OF THE COALVILLE SPECIAL EXPENSES WORKING PARTY** The report of the Strategic Director of Place	**209 - 216**
8.	**EXCLUSION OF PRESS AND PUBLIC** The officers consider that the press and public should be excluded during consideration of the following items in accordance with Section 100(a) of the Local Government Act 1972 as publicity would be likely to result in disclosure	

of exempt or confidential information. Members are reminded that they must have regard to the public interest test and must consider, for each item, whether the public interest in maintaining the exemption from disclosure outweighs the public interest in making the item available.

9. AWARD OF CONTRACT FOR THE PROVISION OF INSURANCE

The report of the Strategic Director of Resources **217 - 230**

Circulation:

Councillor R Blunt (Chair)
Councillor M B Wyatt (Deputy Chair)
Councillor T Gillard
Councillor K Merrie MBE
Councillor N J Rushton
Councillor A C Saffell
Councillor A C Woodman

MINUTES of a meeting of the CABINET held in the Abbey Room, Stenson House, London Road, Coalville, LE67 3FN on TUESDAY, 22 AUGUST 2023

Present: Councillor M B Wyatt (in the Chair)

Councillors T Gillard, K Merrie MBE, A C Saffell and A C Woodman

In Attendance: Councillors S Sheahan

Officers: Mrs A Thomas, Mr A Barton, Mr G Hammons, Ms K Hiller, Mr T Devonshire and Mrs R Wallace

23. APOLOGIES FOR ABSENCE

Apologies were received from Councillors R Blunt and N Rushton.

24. DECLARATION OF INTERESTS

There were no interests declared.

25. PUBLIC QUESTION AND ANSWER SESSION

There were no questions received.

26. MINUTES

The minutes of the meeting held on 25 July 2023 were considered.

It was moved by Councillor T Gillard, seconded by Councillor A C Saffell and

RESOLVED THAT:

The minutes of the meeting held on 25 July 2023 be approved as an accurate record of proceedings.

Reason for decision: To comply with the constitution.

27. MINUTES OF THE COALVILLE SPECIAL EXPENSES WORKING PARTY

The Business and Regeneration Portfolio Holder presented the Report. The Portfolio Holder noted the constitutional status of the Coalville Special Expenses Working Party, a delegated Cabinet function, and informed Members of the recommendations the Working Party had agreed at their meeting in June 2023.

It was moved by Councillor T Gillard, seconded by Councillor A C Saffell and

RESOLVED THAT:

1. The minutes of The Coalville Special Expenses Working Party at Appendix 1 be noted.

2. The Recommendations of the Coalville Special Expenses Working Party be approved.

Reason for Decision: So that the decisions of the Coalville Special Expenses Working Party can be considered.

28. AIR QUALITY SUPPLEMENTARY PLANNING DOCUMENT

The Infrastructure Portfolio Holder presented the report. The Portfolio Holder advised Members on the process through which the report had been produced, noting that drafts of the document had gone before the Cabinet and the Local Plan Committee in September 2022. Following this there had been a public consultation, detailed in Appendix B. There was an unavoidable risk that when central Government produced their own guidance, this document could become obsolete, but should this occur Officers would advise Members on how to proceed in due course.

It was moved by Councillor K Merrie, seconded by Councillor T Gillard and

RESOLVED THAT:

The Local Plan Committee be requested to adopt the Air Quality Supplementary Document attached at Appendix A.

Reason for Decision: The preparation of a Supplementary Planning Document is a Cabinet function.

The meeting commenced at 5.00 pm

The Chairman closed the meeting at 5.05 pm

Chairman's initials

NORTH WEST LEICESTERSHIRE DISTRICT COUNCIL

CABINET – TUESDAY, 19 SEPTEMBER 2023

Title of Report	**REVIEW OF CORPORATE GOVERNANCE POLICIES**	
Presented by	Councillor Nick Rushton Corporate Portfolio Holder PH Briefed [X]	
Background Papers	A&G Agenda and Draft minutes from 26.7.23	**Public Report:** Yes **Key Decision:** Yes
Financial Implications	The annual refresh and update of the policies is good practice and will enhance financial management within the Council. **Signed off by the Section 151 Officer**: Yes	
Legal Implications	Legal implications have been considered in the review of the policies. **Signed off by the Monitoring Officer**: Yes	
Staffing and Corporate Implications	Any staffing or corporate implications are detailed in the policies. **Signed off by the Head of Paid Service:** Yes	
Purpose of Report	To seek Cabinet's comments on and approval of the Council's updated corporate governance policies.	
Reason for Decision	To ensure that the Council has an up to date suite of governance policies in place reflecting the law and best practice.	
Recommendations	**THAT CABINET:** **1. NOTES THE COMMENTS FROM THE AUDIT AND GOVERNANCE COMMITTEE MADE AT ITS MEETING ON 26 JULY 2023.** **2. APPROVES THE CORPORATE GOVERNANCE POLICIES LISTED IN PARAGRAPH 2 OF THE REPORT.**	

1.0 BACKGROUND

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

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

2.0 POLICY REVIEW

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

The main changes to each policy are summarised below:

Anti-Fraud and Corruption Policy

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

Anti-Money Laundering Policy

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

Confidential Reporting (Whistleblowing Policy)

Updated to reflect the Council's address, new management structure and latest terminology within the Council. The update also refers to the Council's external audit firm.

Risk Management Policy

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

RIPA Policy

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

directed surveillance or the use of covert human intelligence sources). Also updated to reflect the Council's new management structure and latest terminology within the Council.

Information Management Policy

Updated to make reference to UK General Data Protection Regulations (GDPR). Update made to the Data Protection Officer role details and update to the Council's address.

Data Protection Policy

Updated to reflect the Council's address.

ICT & Cyber Security Policy

There have been no changes to this Policy.

Local Code of Corporate Governance
Updated in relation to the importance of the role of internal audit in the Council's governance and assurance processes.

The updated policies were considered by the Audit and Governance Committee at their meeting on 26 July 2023. A copy of the report and the draft minutes of the meeting can be accessed via the background papers. A member of the Committee requested that the details of the Council's address on each policy be checked for consistency.

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, Climate Change and zero carbon:	N/A
Consultation/Community Engagement:	N/A
Risks:	The risk management policy is one of the corporate governance policies.

Officer Contact	Anna Crouch Head of Finance Anna.crouch@nwleicestershire.gov.uk

ANTI-FRAUD AND CORRUPTION POLICY

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

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

Version 2.6
June 2023

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

ANTI-FRAUD AND CORRUPTION POLICY

1. INTRODUCTION

1.1 North West Leicestershire District Council has a duty to ensure that it safeguards the public money that it is responsible for. The Council expects the highest standards of conduct and integrity from all that have dealings with it including staff, members, contractors, volunteers and the public. It is committed to the elimination of fraud and corruption and to ensuring that all activities are conducted ethically, honestly and to the highest standard of openness and accountability so as to protect public safety and public money.

1.2 All suspicions or concerns of fraudulent or corrupt practise will be investigated. There will be no distinction made in investigation and action between cases that generate financial benefits and those that do not. Any investigations will not compromise the Council's commitment to Equal Opportunities or the requirements of the Human Rights Act or any other relevant statutory provision.

2. SCOPE

2.1 This policy provides an overview of the measures designed to combat any attempted fraudulent or corrupt act, whether attempted internally or externally. The policy is designed to:

- encourage prevention;
- promote detection;
- ensure effective investigation where suspected fraud or corruption has occurred;
- prosecute offenders where appropriate; and
- recover losses in all instances of fraud or financial irregularity where possible.

3. DEFINITIONS

3.1 Fraud

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

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

Fraud by false representation requires:

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

Fraud by failing to disclose information requires:

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

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

Fraud by abuse of position requires:

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

3.2 Corruption

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

3.3 Bribery

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

3.4 Money Laundering

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

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

5. RESPONSIBILITIES

5.1 Responsibilities of Elected Members

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

5.2 Responsibilities of the Monitoring Officer

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

5.3 Responsibilities of the Section 151 Officer

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

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

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

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

5.4 Responsibilities of Employees

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

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

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

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

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

5.6 Role of the External Auditors

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

5.7 Role of the Public

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

5.8 Conflicts of Interest

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

6. PREVENTION AND DETERRENCE

6.1 Responsibilities of the Senior Management Team

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

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

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

6.2 Role of Internal Audit

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

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

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

6.3 Working with Others and Sharing Information

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

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

6.4 National Fraud Initiative (NFI)

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

6.5 Data Sharing

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

6.6 Training and Awareness

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

6.7 Disciplinary Action

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

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

6.8 Prosecution

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

6.9 Publicity

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

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

7. DETECTION AND INVESTIGATION

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

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

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

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

Action could include:

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

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

8. RAISING CONCERNS

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

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

9. Review

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

APPENDIX A

THE SEVEN PRINCIPLES OF PUBLIC LIFE

Selflessness

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

Integrity

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

Objectivity

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

Accountability

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

Openness

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

Honesty

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

Leadership

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

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

ANTI-MONEY LAUNDERING POLICY

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

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

Version 2.5
June 2023

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

ANTI-MONEY LAUNDERING POLICY

1. INTRODUCTION

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

2. SCOPE OF THE POLICY

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

3. DEFINITION OF MONEY LAUNDERING

3.1 Money laundering is a term designed to cover a number of offences. These offences relateto 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), asamended 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 fromanywhere 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 byor on behalf of another person;
- acquiring, using or possessing criminal property*;
- entering into or being concerned in an arrangement which facilitates the retentionor 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 ofboth criminal property and terrorist property) where there is reasonable grounds for knowledge or suspicion ***; and,
- tipping off or informing someone who is, or is suspected of, being involved in moneylaundering activities, in such a way as to reduce the likelihood of or prejudice an investigation.

*** It is important to note that whilst the disclosure obligations and tipping off offencesin 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 actscarried 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 LaunderingReporting Officer (MLRO). He can be contacted at glenn.hammons@nwleicestershire.gov.uk.

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

6. CLIENT IDENTIFICATION PROCEDURES

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

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

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

7. REPORTING PROCEDURE FOR SUSPICIONS OF MONEY LAUNDERING

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

7.2 Your disclosure should be made to the MLRO using the disclosure form, available on the intranet.

The report must include as much detail as possible including:

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

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

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

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

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

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

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

8.1 Upon receipt of a disclosure report, the MLRO must note the date of receipt on their sectionof the report and acknowledge receipt of it. They should also advise you of the timescalewithin which they expect to respond to you.

8.2 The MLRO will consider the report and any other available internal information they think is relevant, e.g.

- reviewing other transaction patterns and volumes;
- the length of any business relationship involved;
- the number of any one-off transactions and linked one-off transactions;
- any identification evidence held;

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

8.3 Once the MLRO has evaluated the disclosure report and any other relevant information, they must make a timely determination as to whether:

- there is an actual or suspected money laundering taking place; or
- whether there are reasonable grounds to know or suspect that this is the case; and
- whether they need to seek consent from the NCA for a particular transaction toproceed.

8.4 Where the MLRO does so conclude, then they must disclose the matter as soon as practicable to the NCA on their standard report form and in the prescribed manner, unless they 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 nondisclosure, then they must note the report accordingly, they can then immediately give their consent for any ongoing or imminent transactions to proceed. In cases where legal professional privilege may apply, the MLRO must liaise with the Council's Monitoring Officer to decide whether there is a reasonable excuse for not reporting the matter to the NCA.

8.6 Where consent is required from the NCA for a transaction to proceed, then the transaction(s) in question, must not be undertaken or completed until the NCA has given specific consent, or there is deemed consent through the expiration of the relevant time limits in which the NCA must respond, and no response has been received.

8.7 Where the MLRO concludes that there are no reasonable grounds to suspect money laundering then they shall mark the report accordingly and give their consent for any ongoing or imminent transaction(s) to proceed.

8.8 All disclosure reports referred to the MLRO and reports made by them to the NCA must be retained by the MLRO in a confidential file kept for that purpose, for a minimum of five years.

8.9 The MLRO commits a criminal offence if they know or suspect, or have reasonable grounds to do so, through a disclosure being made to them, that another person is engaged in money laundering and does not disclose this as soon as practicable to the NCA.

9. TRAINING

9.1 Officers considered likely to be exposed to suspicious situations, will be made aware of these by their senior officer and provided with appropriate training.

9.2 Additionally, all employees and members will be familiarised with the legal and regulatoryrequirements relating to money laundering and how they affect both the Council and themselves.

9.3 Notwithstanding the paragraphs above, it is duty of officers and members to report all suspicious transactions whether they have received their training or not.

10. REVIEW

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

This page is intentionally left blank

CONFIDENTIAL REPORTING (WHISTLEBLOWING) POLICY

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

Version 2.4
June 2023

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

CONFIDENTIAL REPORTING (WHISTLEBLOWING) POLICY

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

1. INTRODUCTION

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

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

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

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

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

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

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

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

1.6 This policy is designed for workers. Workers include:

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

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

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

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

2. AIMS AND SCOPE OF THE POLICY

2.1 This Policy aims to:

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

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

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

3. SAFEGUARDS - HARASSMENT OR VICTIMISATION

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

supportive of employees and others using this policy.

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

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

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

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

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

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

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

4. CONFIDENTIALITY

4.1 All attempts will be made to ensure any concerns raised will be treated in confidence and to protect the identity of the person making the complaint where they so wish. The Council cannot ensure confidentiality where the individual has themselves informed others of any alleged concerns.

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

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

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

5. ANONYMOUS ALLEGATIONS

5.1 This Policy aims to protect those raising concerns and, therefore, it is hoped that any person raising concerns will do so in their own name whenever possible.

5.2 Whilst any concern will be taken seriously, those expressed anonymously will carry less weight but will be given consideration by the Council; an investigation into the matters raised will be investigated at the discretion of the Council.

5.3 In exercising this discretion, the factors to be taken into account will include:

- the nature and seriousness of the issues raised,
- the apparent credibility of the concern, and
- the probable likelihood of being able to confirm the allegation from attributablesources.

5.4 If the Council does not know who has made an allegation, it will not be possible for the Council to offer reassurance and protection to the individual.

6. UNTRUE ALLEGATIONS

6.1 If an allegation is made in good faith but is not confirmed following an investigation by the Council, no action will be taken against the person making the allegation. This should encourage those who have concerns to raise them in the appropriate manner without fear of any reprisals.

6.2 If, however, an allegation is made frivolously, maliciously or for personal gain, disciplinary action may be taken against the person making that allegation where appropriate.

7. HOW TO RAISE A CONCERN

7.1 Advice and guidance on how to pursue matters of concern may be obtained from the Council's nominated contact points who are:

- Chief Executive:
  Allison.thomas@nwleicestershire.gov.uk
  Telephone 01530454500
- Monitoring Officer:
  elizabeth.warhurst@nwleicestershire.gov.uk
  Telephone 01530 454762
- Interim Section 151 Officer:
  glenn.hammons@nwleicestershire.gov.uk
- Audit Manager:
- kerry.beavis@nwleicestershire.gov.uk
  Telephone 01530 454378

7.2 Concerns may be raised verbally or in writing, to any of the above-named individuals. If raising a concern in writing, it should be addressed to the named individual at the:

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

Clearly mark the envelope "Confidential".

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

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

or via email - Gary.Devlin@azets.co.uk

7.3 Concerns can be raised in the following ways –

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

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

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

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

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

7.9 The individual wishing to raise a concern may invite a trade union representative, professional association representative or a member of staff to be present during any meetings or interviews in connection with the concerns raised, any meetings may be arranged off-site if appropriate.

7.10 If an individual feels unable to raise concerns directly with the Council, they should report the matter to a "prescribed person". This will ensure that their legal rights are protected. The list of prescribed persons can change and so up to date information can be obtained by accessing an online brochure entitled;

"Whistleblowing: list of prescribed people and bodies" available at www.gov.uk

8. HOW THE COUNCIL WILL RESPOND

8.1 The Council will respond to concerns but within the constraints of maintaining confidentiality or observing any legal restrictions. In any event, a confidential record of the steps taken will be kept in accordance with the Data Protection Act 2018.

8.2 The Council may also ask to meet with the individual raising the concern in order to gain further information. Do not forget that testing out concerns is not the same as either accepting or rejecting them. It is sometimes necessary to test out any concerns raised in order to identify how strong any evidence may be.

8.3 Where appropriate, the matters raised may be:

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

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

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

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

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

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

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

information from the individual.

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

8.9 The Council accepts that an individual needs to be assured that the matter has been properly addressed. Thus, subject to legal constraints, we will inform the individual of the outcome of any investigation.

9. THE RESPONSIBLE OFFICER

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

10. HOW THE MATTER CAN BE TAKEN FURTHER

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

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

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

11. Review

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

This page is intentionally left blank

DATA PROTECTION POLICY

Version No.	Author	Date	Summary of Changes
2.0	Nicola Taylor	June 2023	No changes Update Council address & changes to formatting

Version 2.0

June 2023

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

1. INTRODUCTION

Background

1.1 North West Leicestershire District Council (NWLDC) needs to collect person-identifiable information about individuals in order to carry out its functions and fulfil its objectives. Personal data is defined as 'information which relates to a living individual and from which they can be identified, either directly or indirectly'.

1.2 Personal data at NWLDC can include employees (present, past and prospective), service users, contractors and third parties, private and confidential information as well as sensitive information, whether in paper, electronic or other form.

1.3 Irrespective of how information is collected, recorded and processed person-identifiable information must be dealt with properly to ensure compliance with the Data Protection Act 2018 (DPA) and the General Data Protection Regulations 2018 (GDPR).

1.4 The DPA and the GDPR requires NWLDC to comply with the key Data Protection Principles (see Appendix A below) and to notify the Information Commissioner about the data that we hold and why we hold it. This is a formal notification and is renewed annually.

1.5 The DPA and the GDPR gives rights to data subjects (people that we hold information about) to access their own personal information, to have it corrected if wrong, in certain permitted circumstances to ask us to stop using it and to seek damages where we are using it improperly (see Appendix C below).

1.6 The lawful and correct treatment of person-identifiable information by NWLDC is paramount to the success of the organisation and to maintaining the confidence of its service users and employees. This policy will help NWLDC ensure that all person-identifiable information is handled and processed lawfully and correctly.

Data Protection and the GDPR Principles

1.7 NWLDC has a legal obligation to comply with all relevant legislation in respect of data protection and information / IT security. The organisation also has a duty to comply with guidance issued by the Information Commissioners Office.

1.8 All legislation relevant to an individual's right to the confidentiality of their information and the ways in which that can be achieved and maintained are paramount to the Council. Significant penalties can be imposed upon the organisation or its employees for non-compliance.

1.9 The aim of this policy is to outline how the NWLDC meets its legal obligations in safeguarding confidentiality and adheres to information security standards. The obligations within this policy are principally based upon the requirements of the DPA and GDPR, as the key legislative and regulatory provisions governing the security of person-identifiable information.

1.10 Other relevant legislation and guidance referenced and to be read in conjunction with this policy, is outlined together with a brief summary at Appendix B (below).

1.11 GDPR requires Public Authorities to appoint a Data Protection Officer. A data protection officer (DPO) is an enterprise security leadership role required by the General Data Protection Regulation (**GDPR**). Data protection officers are responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR **r**equirements.

2. WHAT INFORMATION IS COVERED?

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

3. POLICY STATEMENT

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

It sets out:

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

4. PRINCIPLES

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

- **To ensure notification;**

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

- **To ensure professionalism;**

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

- **To preserve security;**

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

- **To ensure awareness;**

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

- **Data Subject access;**

  Prompt and informed responses to subject access requests.

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

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

5. SCOPE OF THIS POLICY

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

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

6. POLICY

6.1 The Council 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, the Council will comply with the data protection principles within the DPA and GDPR.

7. DATA PROTECTION POLICIES

Overall responsibilities

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

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

Data Protection Officer's (DPO) responsibilities

7.4 The Data Protection Officer's responsibilities include:

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

- Conduct department reviews to ensure that all departments are compliant and act in accordance with the retention schedule.

Line managers' responsibilities

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

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

General responsibilities

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

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

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

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

8. MONITORING

8.1 Compliance with this policy will be monitored by the Finance and Corporate Governance team, together with internal audit reviews where necessary.

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

9. VALIDITY OF THIS POLICY

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

APPENDIX A
General Data Protection Regulation 2018 – The Data Protection Principles

1. Lawfulness, Fairness and Transparency: Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals.

2. Purpose Limitation: Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

3. Data Minimisation: Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

4. Accuracy: Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

5. Storage Limitation: Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

6. Integrity and Confidentiality: Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

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

APPENDIX B – Summary of Relevant Legislation and Guidance

General Data Protection Regulations (GDPR)

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

Human Rights Act 1998

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

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

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

Freedom of Information Act 2000

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

Regulation of Investigatory Powers Act 2000

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

Crime and Disorder Act 1998

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

The Computer Misuse Act 1990

This Act makes it a criminal offence to access any part of a computer system, programs and/or data that a user is not entitled to access. NWLDC issues each employee with an

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

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

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

APPENDIX C – Individual Rights of the Data Subject

1. The Right to be Informed: Individuals have the right to be provided with clear and concise information about what an organisation does with their personal data. The Concil has published Privacy Notices for each of its departments that outline in detail what data hey collect, how that data is used, the lawful basis for processing the data and for how long date will be retained. These can be found on the Council's 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. Employees 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 it was originally collected or processed , when the Council is are relying on the employee's consent to process the data and that consent is withdrawn, when the Council is relying on legitimate interests as the basis for processing and an employee objects to this processing (so long as there is no overriding legitimate interest to continue this processing), the Council has processed the personal data unlawfully, the Council has to do it to comply with a legal obligation or the Council has 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, every effort will be made to assist. rRquest for erasure can be made 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, the Council is permitted to store the data, but not to use it. This right may apply if the accuracy of an individual's data is being contested and the Council is verifying that accuracy, if the data has been unlawfully processed and rather than invoking the Right to Erasure a restriction is requested instead, if the Council no longer needs the personal data but the indivdual needs the Council to keep it in order to establish, exercise or defend a legal claim, or the indvidual objects to the Council processing your data and the Council is considering whether there are legitimate grounds for processing overrides the request. Individuals 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 them to

move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability. Individuals have the right to request that the Council transfers the data provided to theCouncil 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 the Council is carrying out the processing by automated means (in other words, it excludes paper files). Individuals 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. They have the absolute right to stop r data being used for direct marketing. They 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 the Council's legitimate interests (or those of a third party); however, the right to object is not absolute in these circumstances. Individuals 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 the Council uses profiling of any kind. This information is available on the Council's website at https://www.nwleics.gov.uk/pages/data_protection_notice

To invoke these rights, requests can be submitted to the Council in writing either by email at dpo@nwleicestershire.gov.uk or to:

Whitwick Business Centre
Whitwick Business Park
Stenson Road
Coalville
Leicestershire
LE67 4JP

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

VERSION CONTROL

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

Version Awareness

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

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

This page is intentionally left blank

ICT AND CYBER SECURITY POLICY SEPTEMBER 2023

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

Version 2.5
June 2023

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

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

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

ICT AND CYBER SECURITY POLICY

FORWARD

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

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

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

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

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

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

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

POLICY OBJECTIVES

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

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

(a) the public and all users of the Council's information are confident of the confidentiality, integrity and availability of the information used and produced.

(b) Business damage and interruption caused by cyber security incidents are minimised.

(c) All legislative and regulatory requirements are met.

(d) The Council's information is used responsibly, securely and with integrity at all times and that this applies to manual and electronic information.

The main objectives of this policy are:

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

The strategic approach to cyber security is based on:

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

SCOPE

This Information Technology and Cyber Security Policy will apply to:

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

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

1. SECURITY ORGANISATION

Objective:

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

1.1 Responsibilities

The ICT Manager is responsible for:

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

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

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

Departmental application software is the responsibility of:

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

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

1.2 Acquisition of Information and Communications Technology

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

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

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

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

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

1.3 Security Information Advice

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

1.4 Security Incidents

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

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

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

1.5 Independent Review of Information Security

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

2. SECURITY OF THIRD PARTY ACCESS

Objective:

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

2.1 Identification of Risks from Third Party Connections

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

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

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

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

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

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

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

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

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

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

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

3. ASSETS CONTROL

Objective:

To maintain appropriate protection of organisational assets:

3.1 Inventory of Assets

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

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

4. PERSONNEL SECURITY

Objective:

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

4.1 General

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

All potential recruits will be screened by:

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

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

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

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

4.2 ICT and Cyber Security Training

Objective:

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

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

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

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

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

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

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

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

4.3 Responding to Incidents

Objective:

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

A security incident shall mean:

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

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

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

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

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

5. PHYSICAL AND ENVIRONMENTAL SECURITY

Objective:

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

5.1 Secure Areas

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

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

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

The following specific conditions will apply to such secure areas:

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

5.2 Equipment Security

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

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

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

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

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

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

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

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

5.3 Equipment and Data Destruction

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

All ICT equipment will be disposed of in accordance with the relevant environmental legislation e.g. Waste Electrical and Electronic Equipment (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). The Council 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 suspicions 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.

APPENDIX 1

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	• 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	• 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	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: 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	• Within a single physical location. As determined by the information security officer. • Transfer between establishments within or outside UK**:** 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	• 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	• 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	• 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: 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	• Within a single physical location. As determined by the information security officer.

	• Transfer between establishments within or outside UK**:** 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	• 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.

APPENDIX 2

INTERNET & EMAIL ACCESS – CONDITIONS OF USE

A) Introduction

The purpose of the following Conditions of Use is to safeguard the security and integrity of the Council's Information Technology systems. It outlines personal responsibilities in using these systems..

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

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

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

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

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

In these conditions, 'Internet' means the World Wide Web and 'e-mail' means the use

the Council's internal electronic mail system or the external Internet electronic mail

system.

B) Conditions of Use

1. General

1a. Users may only access Internet and email services using hardware and software installed for that purpose. Users must not interfere with the configuration of the software.

1b. The Council provides a secure login ID and password for all users of Council ICT facilities and this logon ID & password is also used to access the internet and e-mail.

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

1c. Users must treat the information gleaned from the Internet with caution giving due consideration to its unregulated nature. For the purpose of these Conditions of Use, the term 'information' is deemed to include text, data, images or any other material.

1d. Users must not disclose their User-ID's and / or passwords to other persons. All access to internet or e-mail services must be completed using the users own unique User-ID and password. Users will be deemed responsible for all activity logged to their User-ID.

1e. Users must report any known or perceived breach of security to the ICT Service Desk immediately.

1f. A breach of these Conditions of Use may result in disciplinary action and/or criminal proceedings.

2. Internet

2a. Private use of the Internet is permitted but Officers using these facilities for their private purposes must do so outside of their working hours and must adhere to the conditions stated at 2b to 2i at all times. Except for this provision for private use, use of the Internet shall be restricted, specifically during core times, to the proper conduct of the Council's business only. Use of the Internet shall at all times be carried out in a manner which does not prejudice the Council as a responsible provider of public services.

2b. The Internet must not be used to upload *(send)* information in plain text form which might be regarded as sensitive or confidential. This includes both personal and commercially sensitive information which should continue to be sent by conventional means.

2c. Council equipment must not be used for the storage of files or any other information not related to Council business.

2d. the use of Internet Instant Messenger and chat rooms is not permitted.

2e. Users are expressly forbidden from downloading *(receiving*) or viewing from the Internet information, data, images or any other material which is of a pornographic, racist, sexist, homophobic or other discriminatory nature, or extreme political nature, or which incites violence, hatred, illegal activity or abuse in any form. Where possible, such sites have been blocked, however, any user who accidentally accesses such information, data, images or material must immediately notify the ICT Manager or the ICT Service desk. This is to protect you from Condition 1f above.

2g. No software is to be downloaded from the Internet without the prior written consent of either the ICT Manager or the ICT Infrastructure & Security Manager and prior to such downloading, Users must refer to the Council's ICT Security Policy. If the software is to be used on a continuing basis and is subject to any licensing arrangement (e.g. registration of shareware with the publisher), it must be properly registered in accordance with the publisher's requirements and recorded in the Council ICT asset database.

2h. In general terms, any use of the Internet which contravenes any legal Act (for example, The Data Protection Act 1998, The Computer Misuse Act 1990, The Copyrights, Designs and Patents Act 1988), or any internal Council policy is unacceptable.

2i. A Council computer cannot be used for private purposes if, at that time, it is required for use on Council business.

3. <u>E-mail</u>

3a. Use of the Council's e-mail facilities (both internal and external) shall be restricted primarily to the proper conduct of the Council's business only and shall at all times be carried out in a manner which does not prejudice the Council as a responsible provider of public services. The Council recognises that e-mail forms a modern form of communication. To this end, the e-mail facility may be used for occasional [essential] private communications. No charge will be made at present. Frequent or excessively long e-mails may require explanation. Personal e-mail messages must not be retained for longer than absolutely necessary within the Councils e-mail system.

3b. The e-mail facility must not be used to upload *(send)* information in any form which might be regarded as sensitive or confidential. This includes both personal and commercially sensitive information which should continue to be sent by conventional means.

3c. Any user who receives, information, data, images or any other material which is of a pornographic, racist, sexist, homophobic or other discriminatory nature, or extreme political nature, or which incites violence, hatred, illegal activity or abuse in any form such information, data, images or material must immediately notify the ICT Manager or the ICT Service Desk. This is to protect you from Condition 1f above. The item should then be deleted and not forwarded to other people.

3d. Users must not disclose their user-ID and / or passwords to other persons. Users will be deemed responsible for all activity logged to their User-ID. The Council reserves the right to and does monitor both incoming and outgoing e-mails.

3e. The exchange of all electronic mail both internal and external shall at all times be professional and courteous. Official correspondence using the Internet electronic mail must be subject to such management review as is currently in place for posted correspondence.

3f. Where a User has been assigned an e-mail address relating to the Division or Section, it is the User's responsibility to ensure that she/he does not disclose any passwords associated with that e-mail address.

C) Internet and e-mail monitoring.

E-mail

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

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

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

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

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

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

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

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

Internet

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

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

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

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

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

- If the Council suspects that the employee has been spending an excessive amount of time viewing websites that are not work related.

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

When used for private purposes, the Computer, any data held on it or any other activity logs remain the property of the Council and may be accessed at any time by the Council to ensure compliance with all of its statutory, regulatory & internal policy requirements.

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

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

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

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

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

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

✂----------✂

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

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

Print Name _____ Signed _____ Date _____

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

APPENDIX 3

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 SGN 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)

APPENDIX 4

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

INFORMATION MANAGEMENT POLICY

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

Version 1.9
June 2023

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

POLICY STATEMENT

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

1. INTRODUCTION

1.1 The key areas of Information Management are:

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

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

2. PURPOSE OF THE POLICY

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

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

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

3. SCOPE OF THIS POLICY

3.1 This policy, framework and supporting policies apply to:

- All information systems within the organisation (both electronic and paper based);
- All data, information, and records owned by the Council, but also including those held by contractors or partner organisations on behalf of, or as a result of their relationship with, the Council);
- Any information that is owned by other organisations, but may be accessed and used by Council employees;

- Information in whatever storage format and however transmitted (i.e., paper, voice, photo, video, audio or any digital format. It will also cover formats that are developed and used in the future.);
- All employees of the Council, Council members, temporary workers, volunteers, student placements etc;
- The employees of any other organisations having access to Council information, for example, auditors, contractors, and other partner agencies where there is no specific information sharing protocol in place;

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

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

4. PROCEDURES AND GUIDANCE

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

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

5. PRINCIPLES OF INFORMATION MANAGEMENT

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

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

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

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

- Information will be protected against unauthorised access;
- Confidentiality of information will be assured;
- Integrity of information will be maintained;
- Information will be supported by the highest quality data;
- Regulatory and legislative requirements will be met;
- Business continuity plans will be produced, maintained and tested;

- Information security training will be mandatory for all staff;
- All breaches of information security, actual or suspected, will be reported via the Security Incident Procedure and investigated by the Data Protection Officer or Information Management Officer;
- Significant breaches will be handled with support from Human Resources and/or ICT Manager and/or Legal Services;

6. ROLES AND RESPONSIBILITIES

6.1 Information Asset Owners

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

6.1.2 Information Asset Owners will:

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

6.2 Senior Information Risk Owner

6.2.1 From 1 July 2016 the Head of Legal and Support Services became the SIRO.

The SIRO reports to the Corporate Leadership Team (CLT) on all matters relating to Information Management. The SIRO is an officer who is familiar with and takes ownership of the organisation's information risk policy, and acts as advocate for information risk

6.3 Data Protection Officer

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

The DPO Information Management responsibilities include:

- Implementing information management procedures and processes for the organisation;
- Raising awareness about information management to all staff;
- Ensuring that training is provided annually and is completed by all staff;

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

6.4 Information Governance

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

- Assists the Senior Information Risk Owner in the implementation of their key responsibilities and any other matters as deemed appropriate and necessary;
- Maintains an awareness of information management issues within the Council;
- Reviews and update the information management policy in line with local and national requirements;
- Reviews and audit all procedures relating to this policy where appropriate on an ad-hoc basis;
- Ensures 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:

- Formulating and implementing ICT related policies and the creating supporting procedures;
- Developing, implementing and managing robust ICT security arrangements in line with best industry practice, legislation, and statutory requirements;
- Ensuring 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 are responsible for ensuring that the Information Management Policy is implemented within their team. All managers will ensure that:

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

- Their responsibility for the information that they use;
- Where to get advice on security issues and how to report suspected security incidents.

6.7 Staff

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

- Policy/strategy and procedure manuals;
- Their line manager;
- The Legal Team;
- Specific training courses;
- Other communication methods, for example, team meetings; and Staff Intranet.

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

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

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

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

7. MAIN THEMES

7.1 Openness

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

7.2 Legal Compliance

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

the Freedom of Information Act 2000, the Environmental Information Regulations 2004, and the Humans Rights Act 1998.

7.3 Information Security

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

7.4 Information and Records Management

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

7.5 Information Quality Assurance

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

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

7.6 Partnerships and Information Sharing

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

8. RISK

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

9. TRAINING

9.1 Appropriate training will be mandatory for all staff.

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

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

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

10.1 COMPLIANCE

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

11. FEES AND CHARGES

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

12. COMPLAINTS

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

- DPO@NWLeicestershire.gov.uk (personal data requests)
- FOI@NWLeicestershire.gov.uk (non-personal information request)
- Data Protection Officer
  North West Leicestershire District Council
  Whitwick Business Centre
  Stenson Road
  Coalville
  Leicestershire
  LE67 4JP

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

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

13. EQUALITIES IMPACT ASSESSMENT

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

14. REVIEW OF POLICY

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

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

LOCAL CODE OF CORPORATE GOVERNANCE

Version No.	Author	Date	Summary of Changes
1		2009	
2	Tracy Bingham	October 2017	
3	Tracy Bingham	May 2020	
4	Dan Bates	June 2021	
5	Mark Walker	May 2022	
6	Glenn Hammons	July 2023	New section on the current challenges facing the Council Changes to formatting

Version 6
July 2023

	Contents	Page No.
1.	Introduction	3
2.	Summary of Commitment	5
3.	Fundamental Principles of Corporate Governance	5

NORTH WEST LEICESTERSHIRE DISTRICT COUNCIL

Local Code of Corporate Governance

1 INTRODUCTION

1.1 In 2014, the Chartered Institute of Public Finance and Accountancy (CIPFA) and the International Federation of Accountants (IFAC) collaborated to produce The International Framework: Good Governance in the Public Sector. The International Framework defines governance as comprising the arrangements put in place to ensure that intended outcomes for stakeholders are defined and achieved. It states that in order to deliver good governance in the public sector, both governing bodies and individuals working for public sector entities must try to achieve their entity's objectives while acting in the public interest at all times.

1.2 The Chartered Institute of Public Finance and Accountancy in association with SOLACE have published their Framework entitled 'Delivering Good Governance in Local Government 2016'.

1.3 The diagram below[1] 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).

1.7 These seven core principles, also known as the Nolan Principles - The Seven Principles of Public Life, apply to anyone who works as a public office-holder. This includes all those who are elected or appointed to public office, nationally and locally, and all people appointed to work in the Civil Service, local government, the police, courts and probation services, non-departmental public bodies (NDPBs), and in the health, education, social and care services. A link to the Government website setting out the principles is below:

https://www.gov.uk/government/publications/the-7-principles-of-public-life/the7-principles-of-public-life--2

2 SUMMARY OF COMMITMENT

2.1 By adopting this Local Code of Corporate Governance, we are responding to the CIPFA/SOLACE Joint Working Group Guidance and Framework entitled 'Delivering Good Governance in Local Government'.

2.2 In doing so we will:

- Accept the core principles set out in section 3 below as the basis for our Corporate Governance arrangements.
- Publish an Annual Governance Assurance Statement with the Council's Statement of Accounts.
- Draw up Action Plans of improvements to our corporate governance arrangements, such plans to be monitored by the Audit and Governance Committee.

3 FUNDAMENTAL PRINCIPLES OF CORPORATE GOVERNANCE

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

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

The Council is committed to:

Behaving with Integrity

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

Demonstrating strong commitment and ethical values

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

Respecting the rule of law

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

Principle B – Ensuring openness and comprehensive stakeholder engagement

The Council is committed to:

Openness

Ensuring an open culture through demonstrating, documenting and communicating the organisation's commitment to openness

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

Engaging comprehensively with institutional stakeholders

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

Engaging stakeholders effectively, including individual citizens and service users

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

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

The Council is committed to:

Defining outcomes

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

Sustainable economic, social and environmental benefits

- Considering and balancing the combined economic, social and environmental impact of policies, plans and decisions when taking decisions about service provision.
- Taking a longer-term view with regard to decision making, taking account of risk and acting transparently where there are potential conflicts between the organisation's intended outcomes and short-term factors such as the political cycle or financial constraints.
- Ensuring fair access to services.
- Determining the wider public interest associated with balancing conflicting interests between achieving the various economic, social and environmental benefits, through consultation where possible, in order to ensure appropriate trade-offs.

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

The Council is committed to:

Determining interventions

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

Planning interventions

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

Optimising achievement of intended outcomes

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

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

The Council is committed to:

Developing the entity's capacity

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

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

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

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

The Council is committed to:

Managing risk

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

Managing performance

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

Robust internal control

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

Managing Data

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

Strong Public Financial Management

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

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

The Council is committed to:

Implementing good practice in transparency

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

Implementing good practice in reporting

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

Assurance and effective accountability

- Ensuring that recommendations for corrective action made by external audit are acted upon.
- Ensuring an effective internal audit service with direct access to Audit and Governance Committee members is in place which provides assurance with regard to governance arrangements and recommendations are acted upon.
- Welcoming peer challenge, reviews and inspections from regulatory bodies and implementing recommendations.
- Gaining assurance on risks associated with delivering services through third parties and that this is evidenced in the annual governance statement.
- Ensuring that when working in partnership, arrangements for accountability are clear and that the need for wider public accountability has been recognised and met.

This page is intentionally left blank

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

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

Version 1.4
June 2023

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

CORPORATE POLICY AND PROCEDURE ON THE REGULATION OF INVESTIGATORY POWERS ACT 2000 AND THE INVESTOGATORY 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 INTELLEGENCE SOURCES

3.1 A person is a **Covert Human Intelligence Source** (**CHIS**) if he or she establishes or maintains a personal or other relationship with another person in order to covertly obtain or disclose information.

3.2 RIPA sets out special rules relating to the management and use of information supplied by a **CHIS** and a duty of care is owed to the **CHIS** in how the information is used.

3.3 The conduct or use of a **CHIS** requires prior authorisation. Again, the ground on which a **CHIS** may be used by a Local Authority is "for the purpose of preventing or detecting crime or of preventing disorder."

3.4 A RIPA authorisation may not be required in circumstances where members of the public volunteer information to the Council as part of their normal civic responsibilities, however, this will depend on how the information has been obtained. If the person has obtained the information as an 'insider' i.e. in the course of a personal or other relationship or "as a result of the existence of such a relationship" then the person is likely to be a **CHIS,** even if the relationship was not formed or maintained for that purpose.

3.5 If the person has obtained the information as an outside observer then he or she is not a **CHIS**.

3.6 Where contact numbers are set up by the Council to receive information then it is unlikely that persons reporting information will be **CHISs** and similarly, people who complain about anti- social behaviour, and are asked to keep a diary, will not normally

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

Juvenile CHISs

3.7 Special safeguards apply to the use or conduct of juveniles, that is, those under 18 years old, as a **CHIS**. On no occasion should the use or conduct of a **CHIS** under 16 years of age be authorised to give information against their parents or any person who has parental responsibility for them. In other cases, authorisations should not be granted unless the special provisions, contained within the Regulation of Investigatory Powers (Juveniles) Order 2000 (as amended), are satisfied.

3.8 Authorisations for juvenile sources should be granted by those listed in the table at Annex A of the Home Office Covert Human Intelligence Sources Revised Code of Practice (latest edition at time of writing was August 2018). In this Council, only the Chief Executive may authorise the use of a juvenile or vulnerable individual as a CHIS. The duration of such an authorisation is four months from the time of grant or renewal (instead of twelve months), and the authorisation should be subject to at least monthly review. For the purpose of these rules, the age test is applied at the time of the grant or renewal of the authorisation.

4. OPEN SOURCE (ONLINE) COVERT ACTIVITY

4.1 The use of the internet may be required to gather information during an operation, which may amount to **directed surveillance**. The Home Office Covert Surveillance and Property Interference Revised Code of Practice (latest edition at time of writing was August 2018) advises that simple reconnaissance of websites, that is, preliminary examination with a view to establishing whether a site or its contents are of interest, is unlikely to interfere with a person's reasonably held expectation of privacy and therefore is not likely to require a **directed surveillance** authorisation. However, where there is an intention to use the internet as part of an investigation and private information is likely to be obtained, a RIPA authorisation should be considered. When conducting an investigation which involves the use of the internet factors to consider are:

- officers must not create a false identity in order to "befriend" individuals on social networks without an authorisation under RIPA;
- officers viewing an individual's public profile on a social network should do so only to the minimum degree necessary and proportionate in order to obtain evidence to support or refute the suspicions or allegations under investigation;
- repeated viewing of open profiles on social networks to gather evidence or to monitor an individual's status, must only take place once a RIPA authorisation has been granted and approved by a Magistrate; and
- officers should be aware that it may not be possible to verify the accuracy of information on social networks and, if such information is to be used as evidence, take reasonable steps to ensure its validity.

4.2 Further, where an investigator may need to communicate covertly online, for example, contacting individuals using social media websites without disclosing his or her identity, a **CHIS** authorisation should be considered.

5. USE OF PERSONAL DEVICES FOR BUSINESS USE

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

6. THE COUNCIL OWNED DRONE

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

7. LOCAL AUTHORIY DIRECTED SURVEILLANCE CRIME THRESHOLD

7.1 A **Crime Threshold** applies to the authorisation of **directed surveillance** by Local Authorities under RIPA (see article 7A of the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010). This **Crime Threshold** does not apply to the authorisation of a **CHIS** by a Local Authority.

7.2 Local Authorities can only authorise use of **directed surveillance** under RIPA for the purpose of preventing or detecting criminal offences or disorder associated with criminal offences that are:

7.2.1 punishable, whether on summary conviction or on indictment, by a maximum term of at least six months imprisonment; or

7.2.2 relate to the underage sale of alcohol or tobacco.

7.3 If the **Crime Threshold** is not met, though surveillance is still required, a Non-RIPA form should be completed. A Non-RIPA form requires the applicant officer to consider necessity and proportionality as per a RIPA authorisation, however, there is no requirement for approval by a Justice of the Peace.

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

Stage 1 - Request for Authorisation

8.1 **Directed surveillance** or the use of a **CHIS** can only be authorised by a Local Authority if the authorisation is *necessary* for the purpose of preventing or detecting crime or preventing disorder and the authorised surveillance is *proportionate* to what is sought to be achieved by carrying the surveillance out. When authorising the use of a **CHIS** arrangements also need to be in place for management of the **CHIS** and to ensure the security and welfare of the **CHIS**.

8.2 For **directed surveillance** or the use of a **CHIS**, only the approved RIPA forms, available on the Home Office website

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

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

8.3 If in doubt about the process to be followed or the information required in the form, an applicant officer should always seek the advice of the Head of Legal and Support Services or the Audit Manager before applying for an authorisation under RIPA.

8.4 The applicant officer will be responsible for ensuring that copies of all forms are forwarded to the Audit Manager within seven days of issue. As a control measure the Audit Manager will supply the applicant officer with a referenced copy of the authorisation which they should keep in their department in secure storage. Officers should ensure that material passing between them is sent in such a way that it cannot be read or intercepted by other people.

Stage 2 - Considering an Application for Authorisation

8.5 **Directed surveillance** or use of a **CHIS** can only be lawfully carried out if properly authorised and carried out in strict accordance with the terms of the authorisation.

8.6 The Secretary of State has specified by statutory instrument (the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010)) that, for any district council in England, Directors, Heads of Service or Service Managers or equivalent are designated persons for the purpose of s.28 and s.29 of RIPA, that is, they may act as Authorising Officers for the purpose of authorising applications for **directed surveillance** or the use of a **CHIS**. In this Council, the Chief Executive, the Directors and Heads of Service are designated to act as Authorising Officers under the Constitution (Part 2, Sec G4, Para 1.5).

8.7 Before signing a form seeking authorisation, the Authorising Officer must have regard to this Policy and Procedure, to any relevant Code of Practice, to any advice from the Head of Legal and Support Services or the Audit Manager and to any other relevant guidance.

8.8 The Authorising Officer must also satisfy himself / herself that the surveillance proposed in the application is:

8.8.1 in *accordance with the law*;

8.8.2 *necessary* in the circumstances of the particular case on the ground of preventing or detecting crime or preventing disorder; and

8.8.3 *proportionate* to what it seeks to achieve.

8.9 In considering whether or not the proposed surveillance is proportionate, the Authorising Officer will need to consider:

8.9.1 The seriousness of the crime or disorder which the surveillance seeks to detect and weigh this against the type and extent of surveillance proposed. For minor offences, it may be that surveillance is never proportionate; and

8.9.2 whether there are other more non- intrusive ways of achieving the desired outcome. If there are none, the Authorising Officer will need to consider whether the proposed surveillance is no more than necessary to achieve the objective, as the least intrusive method will be considered proportionate by the courts.

8.10 The Authorising Officer will also need to take into account the risk of intrusion into the privacy of persons other than the specified subject of the surveillance. This is known as "**collateral intrusion**". Measures must be taken whenever practicable to avoid or minimise, so far as practicable, **collateral intrusion**.

8.11 When authorising the conduct or use of a **CHIS** the Authorising Officer must also be satisfied that appropriate arrangements are in place for the management and oversight of the **CHIS**. This must address health and safety issues through a risk assessment. The Authorising Officer must also have regard to any adverse impact on community confidence that may result from the use or conduct of the information obtained.

8.12 The authorisation does not take effect until a Justice of the Peace has made an order approving the grant of the authorisation.

Stage 3 - Judicial Approval

8.13 If the Authorising Officer is satisfied that the surveillance is *necessary* and *proportionate,* they will instruct Legal Services to seek approval from a Justice of the Peace sitting at the Magistrates' Court.

8.14 Legal Services will request a hearing date from the Court. The time taken to obtain a heating date from the Court will need to be taken into account when scheduling any proposed surveillance.

8.15 Urgent approvals should not be necessary.

8.16 If the approval is urgent and cannot be handled the next working day then the applicant officer should:

8.16.1 phone the Court's out of hours legal staff contact. You will be asked about the basic facts and urgency of the authorisation. If the police are involved in the investigation you will need to address why the police cannot authorise the application.

8.16.2 If urgency is agreed, then arrangements will be made for a suitable Magistrate to consider the application. You will be told where to attend and give evidence.

8.16.3 Attend the hearing as directed with two copies of the signed RIPA authorisation form.

8.17 At the hearing the Council will provide the Court with a copy of the authorisation signed by the Authorising Officer, together with any supporting documents relevant to the matter showing the necessity and proportionality of the authorisation and which contain all the information relied upon. Also included will be a summary of the circumstances of the case.

8.18 The hearing will be in private heard by a single Justice of the Peace (Magistrate / District Judge) who will read and consider the application.

8.19 On reviewing the papers and hearing the application the Justice of the Peace will determine whether they are satisfied that there were, at the time the authorisation was granted, and continue to be reasonable grounds for believing that the authorisation is

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

8.20 For authorisations for the use of a **CHIS** the Justice of the Peace will also need to be satisfied that there were and are reasonable grounds for believing appropriate arrangements are in place for the management and oversight of the **CHIS**.

8.21 The Justice of the Peace may ask questions of the Council in order to satisfy themselves of the necessity and proportionality of the request.

8.22 In considering the application the Justice of the Peace may decide to:

8.22.1 grant an Order approving the authorisation or renewal. The authorisation or renewal will then take effect and the Local Authority may proceed to use surveillance in accordance with the authorisation;

8.22.2 refuse to approve the authorisation or renewal. The RIPA authorisation will not take effect and the Local Authority may not use the proposed surveillance. Where an application has been refused the Council may wish to consider the reasons for that refusal. For example, a technical error in the form may be remedied without the need to go through the internal authorisation process again. The Council may then wish to reapply for judicial approval once those errors have been remedied;

8.22.3 refuse to approve the grant or renewal and quash the authorisation or notice. A Justice of the Peace must not exercise its power to quash an authorisation unless the applicant (the Council) has had at least two business days' notice from the date of the refusal in which to make representations.

Stage 4 - Duration and Review

8.23 If the Justice of the Peace approves the authorisation, the authorisation will last, in the case of **directed surveillance**, a period of 3 months and, in the case of a **CHIS**, a period of 12 months.

8.24 Authorising Officers must then conduct regular reviews of authorisations granted in order to assess the need for the surveillance to continue. Reviews should be conducted on a monthly basis as a minimum. The Authorising Officer may decide that reviews should be conducted more frequently, particularly where a high level of collateral intrusion is likely.

8.25 A review involves consultation with the applicant officer and any other persons involved in the surveillance. The applicant officer must give sufficient information about the surveillance and any information obtained by the surveillance for the Authorising Officer to be satisfied that the authorised surveillance should continue. Applicant officers should be pro-active in preparing reports to assist Authorising Officers carry out reviews.

Stage 5 - Renewals

8.26 If it appears that the surveillance will continue to be *necessary* and *proportionate* beyond the 3 month period for **directed surveillance** or 12 months for use of a **CHIS**, the authorisation must be renewed.

8.27 An application for renewal should be made by the applicant officer by completing the appropriate form which is available from the Home Office website (https://www.gov.uk/government/collections/ripa-forms--2). This form should then be submitted to the Authorising Officer who must then consider the matter afresh, including taking into account the benefits of the surveillance to date and any collateral intrusion that has occurred.

8.28 The Authorising Officer must be satisfied that it is *necessary* and *proportionate* for the authorisation to continue and that the **Crime Threshold** continues to be met. The authorisation for renewal must then be approved by a Justice of the Peace for it to take effect.

8.29 An authorisation may be renewed and approved before the initial authorisation ceases to have effect but the renewal takes effect from the time at which the authorisation would have expired. If necessary, a renewal can be granted more than once.

Stage 6 - Cancellations

8.30 The Authorising Officer who granted or last renewed the authorisation must cancel the authorisation if the grounds for granting (or renewing) no longer apply or if the authorisation is no longer *necessary* or *proportionate*.

8.31 An authorisation can be cancelled on the initiative of the Authorising Officer following a periodic review or after receiving an application for cancellation from the applicant officer. Forms for the cancellation of **directed surveillance** and use of a **CHIS** are available on the Home Office website

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

9. COMMUNICATIONS DATA

9.1 The term "**communications data**" includes the "who", "when", "where", and "how" of a communication but not the content i.e. what was said or written. It includes the way in which, and by what method, a person or thing communicates with another person or thing. It excludes anything within a communication including text, audio and video that reveals the meaning, other than inferred meaning, of the communication.

9.2 It can include the address to which a letter is sent, the time and duration of a communication, the telephone number or e-mail address of the originator and recipient, and the location of the device from which the communication was made. It covers electronic communications including internet access, internet telephony, instant messaging and the use of applications. It also includes postal services.

9.3 The acquisition of **communications data** is permitted under Part 3 of the IPA and will be a justifiable interference with an individual's human rights under the European Convention on Human Rights only if the conduct being authorised or required to take place is *necessary* for the purposes of a specific investigation or operation, *proportionate* and *in accordance with law*.

9.4 Training should be made available to all those who participate in the acquisition and disclosure of **communications data**.

9.5 The Home Office has published the "Communications Data Code of Practice" (latest edition at time of writing was November 2018). This code should be readily available to persons involved in the acquisition of **communications data** under the IPA and persons exercising any functions to which this code relates must have regard to the code.

9.6 The IPA stipulates that conduct to be authorised must be *necessary* for one or more of the purposes set out in the IPA. For Local Authorities this purpose is "for the applicable crime purpose" which means:

9.6.1 where the **communications data** is wholly or partly events data (events data covers information about time-bound events taking place across a telecommunication system at a time interval, for example, information tracing the origin or destination of a communication that is, or has been, in transmission), the purpose of preventing or detecting serious crime; or

9.6.2 in any other case, the purpose of preventing or detecting crime or of preventing disorder.

9.7 "Serious Crime" means:

9.7.1 an offence for which an adult is capable of being sentenced to one year or more in prison;

9.7.2 any offence involving violence, resulting in a substantial financial gain or involving conduct by a large group of persons in pursuit of a common goal;

9.7.3 any offence committed by a body corporate;

9.7.4 any offence which involves the sending of a communication or a breach of privacy; or

9.7.5 an offence which involves, as an integral part of it, or the sending of a communication or breach of a person's privacy.

9.8 A Local Authority may not make an application that requires the processing or disclosure of internet connection records for any purpose.

10. AUTHORISATION PROCESS - COMMUNICATIONS DATA

10.1 Acquisition of **communications data** under the IPA involves four roles:

10.1.1 The Applicant Officer - The applicant officer is a person involved in conducting or assisting an investigation or operation within a relevant public authority who makes an application in writing or electronically for the acquisition of **communications data**;

10.1.2 The Single Point of Contact (SPoC) - The SPoC is an individual trained to facilitate the lawful acquisition of **communications data** and effective co-operation between a public authority, the Office for Communications Data Authorisations (OCDA) and telecommunications operators and postal operators. To become accredited an individual must complete a course of training appropriate for the role of a SPoC and have been issued the relevant SPoC unique identifier. The Home Office provides authentication services to enable telecommunications operators and postal operators to validate SPoC credentials;

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

10.1.4 The Authorising Individual - **Communications data** applications can be authorised by three separate categories of individual depending on the circumstances of the specific case. The Authorising Individual for Local Authorities is the authorising officer in the OCDA. Section 60A of the IPA confers power on the IPC to authorise certain applications for **communications data**. In practice the IPC will delegate these functions to his staff. These staff will sit in a body which is known as the OCDA.

10.2 An authorisation provides for persons within a public authority to engage in conduct relating to a postal service or telecommunication system, or to data derived from such a telecommunication system, to obtain **communications data**. The following types of conduct may be authorised:

10.2.1 conduct to acquire **communications data** - which may include the public authority obtaining **communications data** themselves or asking any person believed to be in possession of or capable of obtaining the **communications data** to obtain and disclose it; and/or

10.2.2 the giving of a notice - allowing the public authority to require by a notice a telecommunications operator to obtain and disclose the required data.

Stage 1 - Making an Application

10.3 Before public authorities can acquire **communications data**, authorisation must be given by an Authorising Individual. An application for that authorisation must include an explanation of the necessity of the application.

10.4 Necessity should be a short explanation of the investigation or operation, the person and the **communications data** and how these three link together. The application must establish the link between the three aspects to be able to demonstrate the acquisition of **communications data** is necessary for the statutory purpose specified.

10.5 When granting an authorisation the authorising individual must also believe that conduct to be proportionate to what is sought to be achieved by obtaining the specified **communications data** – that the conduct is no more than is required in the circumstances. This involves balancing the extent of the interference with an individual's rights and freedoms against a specific benefit to the investigation or operation being undertaken by a relevant public authority in the public interest.

10.6 As well as consideration of the rights of the individual whose data is to be acquired consideration must also be given to any actual or potential infringement of the privacy and other rights of individuals who are not the subject of the investigation or operation.

10.7 The applicant officer will complete an application form setting out for consideration the necessity and proportionality of a specific requirement for acquiring **communications data**.

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

Stage - 2 Consultation with the Single Point of Contact

10.9 A SPoC must be consulted on all Local Authority applications before they are authorised.

10.10 Amongst other things the SPoC will:

10.10.1 assess whether the acquisition of specific **communications data** from a telecommunications operator or postal operator is reasonably practicable or whether the specific data required is inextricably linked to other data; and

10.10.2 advise applicants on the most appropriate methodology for acquisition of data where the data sought engages a number of telecommunications operators or postal operators.

10.11 The National Anti-Fraud Network ('NAFN') is hosted by Tameside Metropolitan Borough Council.

10.12 In accordance with section 73 of the IPA, all Local Authorities who wish to acquire **communications data** under the IPA must be party to a collaboration agreement. In practice this means they will be required to become members of NAFN and use NAFN's shared SPoC services. Applicant officers within Local Authorities are therefore required to consult a NAFN SPoC throughout the application process. The accredited SPoCs at NAFN will scrutinise the applications independently. They will provide advice to the Local Authority ensuring it acts in an informed and lawful manner.

10.13 In addition to being considered by a NAFN SPoC, the local authority making the application must ensure someone of at least the rank of the senior responsible officer in the local authority is aware the application is being made before it is submitted to an authorising officer in OCDA. The local authority senior responsible officer must be satisfied that the officer(s) verifying the application is (are) of an appropriate rank and must inform NAFN of such nominations. In this Council the Chief Executive is the Senior Responsible Officer and the officers notified to the NAFN (notified in March 2019) as able to verify applications are the Head of Legal and Support Services and the Audit Manager.

10.14 NAFN will be responsible for submitting the application to OCDA on behalf of the local authority.

Stage 3 - Authorisation of Applications

10.15 The (OCDA) performs this function on behalf of the IPC. An authorising officer in OCDA can 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 Support Services will be responsible for:

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

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

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

11.3 The Audit Manager will be responsible for:

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

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

11.3.3 allocating reference numbers to authorisations.

12. WORKING WITH OTHER AGENCIES

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

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

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

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

13. OTHER SOURCES OF INFORMATION

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

14. RECORDS MANAGEMENT

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

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

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

Service Records

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

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

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

14.4.3 the frequency of reviews prescribed by the Authorising Officer;

14.4.4 a record of the result of each review;

14.4.5 a copy of any renewal of an authorisation and any supporting documentation submitted when the renewal was requested;

14.4.6 the date and time when any instruction was given by the Authorising Officer, including cancellation of such authorisation;

14.4.7 a copy of the order approving or otherwise the grant or renewal of an authorisation from a Justice of the Peace; and

14.4.8 the required date of destruction and when this was completed.

Central Record Maintained by the Audit Manager

14.5 A central record of all authorisation forms, whether authorised or rejected, is kept by the Audit Manager. The central record must be readily available for inspection on request by the Investigatory Powers Commissioner.

14.6 The central record must be updated whenever an authorisation is granted, reviewed, renewed or cancelled. Records will be reviewed after a period of 6 years from the date on which the relevant criminal or civil proceedings file is closed for archive and deleted when no longer necessary.

14.7 The central record must contain the following information:

14.7.1 the type of authorisation;

14.7.2 the date on which the authorisation was given;

14.7.3 name / rank of the Authorising Officer;

14.7.4 details of attendances at the Magistrates' Court to include date of attendances at court, the determining Justice of the Peace, the decision of the Justice of the Peace and the time and date of that decision;

14.7.5 the unique reference number (URN) of the investigation / operation. This will be issued by the Audit Manager when a new application is entered in the Central Record. The applicant officer will be informed accordingly and should use the same URN when requesting a renewal or cancellation;

14.7.6 the title of the investigation / operation, including a brief description and names of the subjects, if known;

14.7.7 if the authorisation was renewed, when it was renewed and who authorised the renewal, including the name and rank / grade of the Authorising Officer;

14.7.8 whether the investigation / operation is likely to result in the obtaining of **confidential information** (information is confidential if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation. Examples might include consultations between a health professional and a patient, information from a patient's medical records; or matters subject to legal privilege);

14.7.9 if the authorisation was reviewed, when it was reviewed and who authorised the review, including the name and rank / grade of the Authorising Officer;

14.7.10 the date and time that the authorisation was cancelled.

14.8 It should also contain a comments section enabling oversight remarks to be included for analytical purposes.

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

Retention and Destruction of Material

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

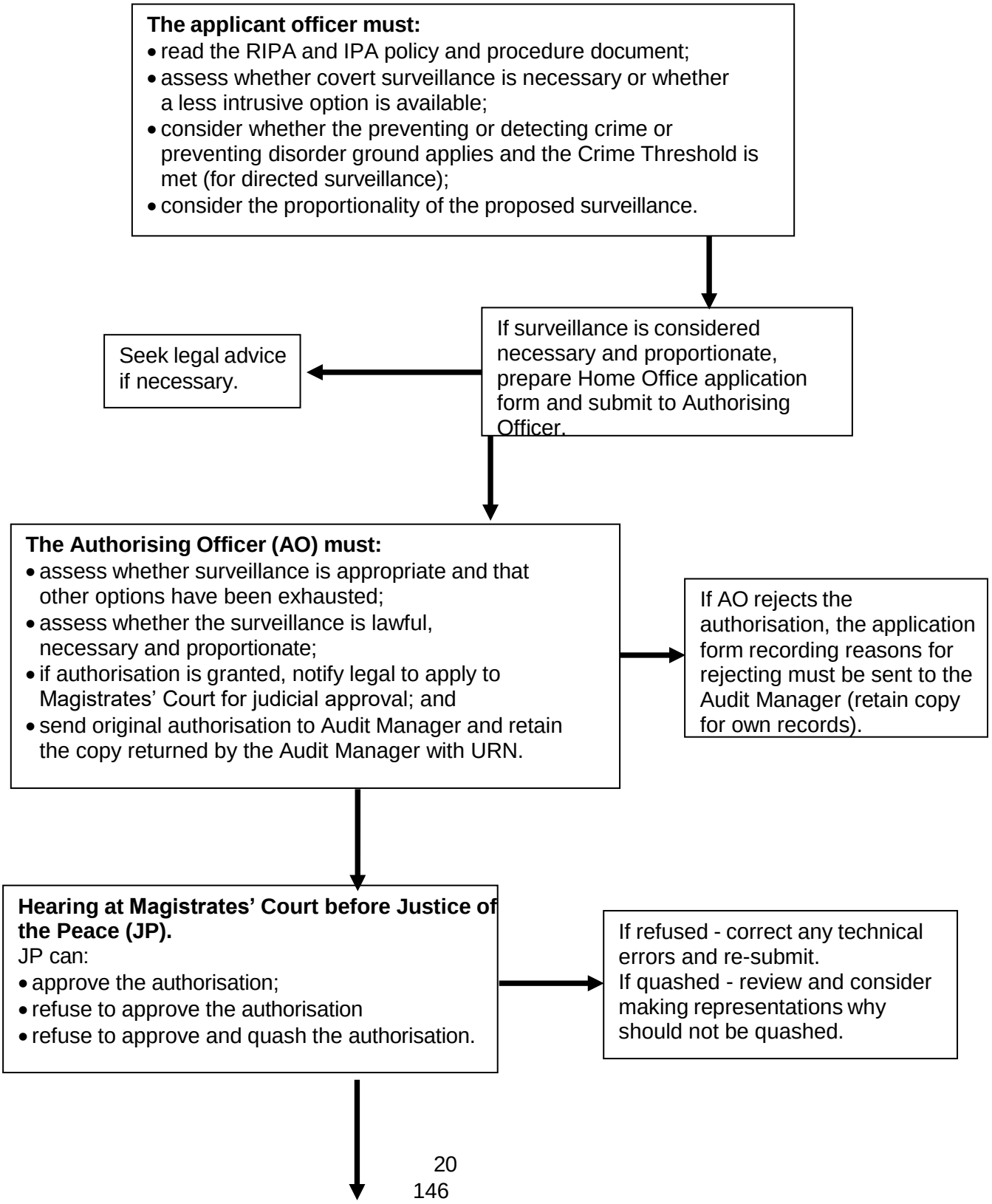
15. REVISION HISTORY

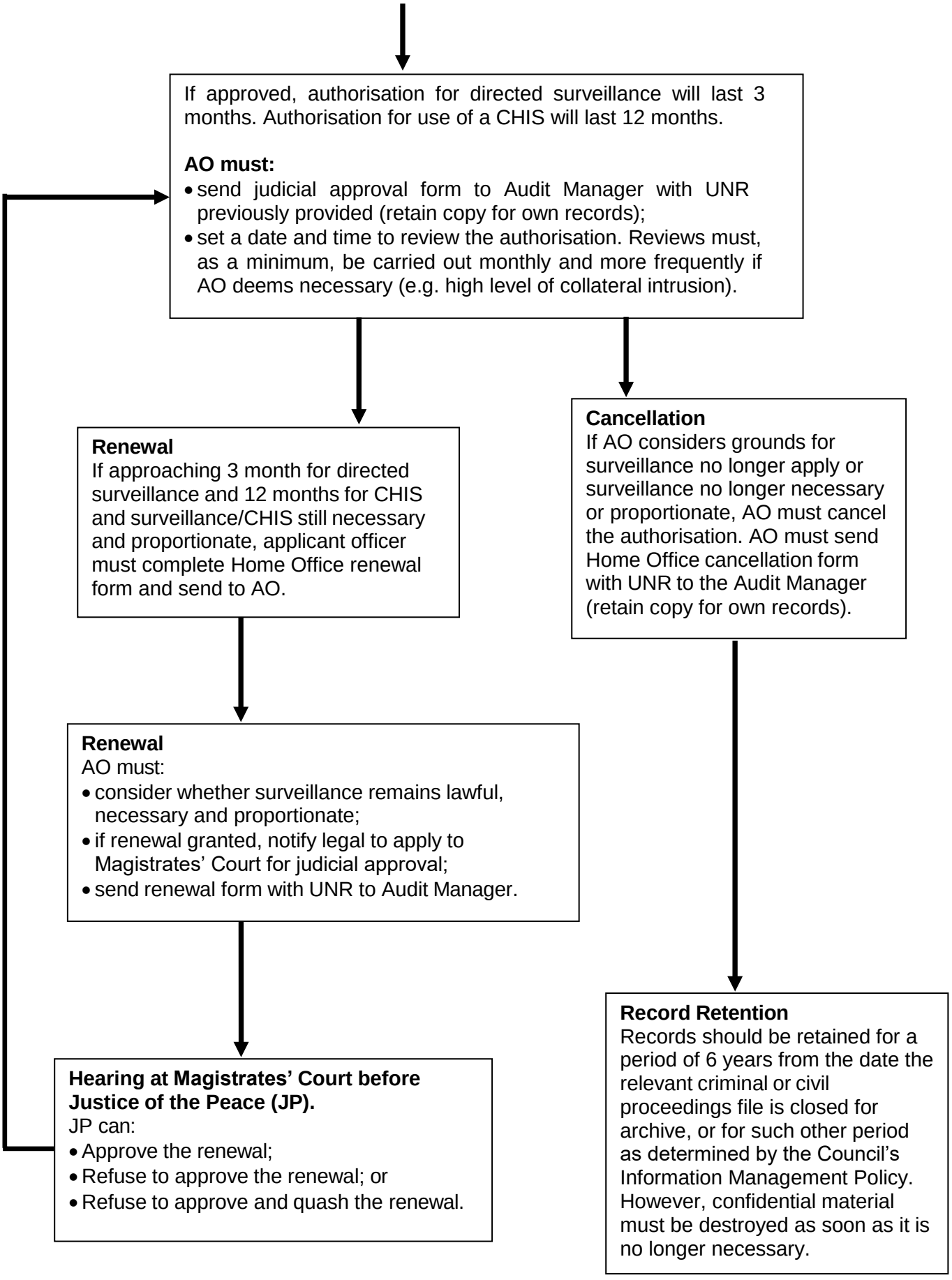
Date	**Action**
December 2006	ASG Revised
May 2009	ASG Reviewed
June 2010	AW Reviewed and updated
March 2012	ASG Revised
October 2012	HO Guidance issued
September 2013	RH Reviewed and updated
October 2015	DMG Reviewed and updated
9 December 2015	Approved by Audit and Governance Committee
12 January 2016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

APPENDIX 1

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)




If approved, authorisation for directed surveillance will last 3 months. Authorisation for use of a CHIS will last 12 months.
AO must:
• send judicial approval form to Audit Manager with UNR previously provided (retain copy for own records);
• set a date and time to review the authorisation. Reviews must, as a minimum, be carried out monthly and more frequently if AO deems necessary (e.g. high level of collateral intrusion).
Renewal
If approaching 3 month for directed surveillance and 12 months for CHIS and surveillance/CHIS still necessary and proportionate, applicant officer must complete Home Office renewal form and send to AO.
Cancellation
If AO considers grounds for surveillance no longer apply or surveillance no longer necessary or proportionate, AO must cancel the authorisation. AO must send Home Office cancellation form with UNR to the Audit Manager (retain copy for own records).
Renewal
AO must:
• consider whether surveillance remains lawful, necessary and proportionate;
• if renewal granted, notify legal to apply to Magistrates' Court for judicial approval;
• send renewal form with UNR to Audit Manager.
Hearing at Magistrates' Court before Justice of the Peace (JP).
JP can:
• Approve the renewal;
• Refuse to approve the renewal; or
• Refuse to approve and quash the renewal.
Record Retention
Records should be retained for a period of 6 years from the date the relevant criminal or civil proceedings file is closed for archive, or for such other period as determined by the Council's Information Management Policy. However, confidential material must be destroyed as soon as it is no longer necessary.

APPENDIX 1

IPA - COMMUNICATIONS DATA AUTHORISATION PROCESS

The applicant officer must:
- read the RIPA and IPA policy and procedure document;
- assess whether communications data is necessary and proportionate; and
- consider whether the applicable crime purpose applies.

If communications data is considered necessary and proportionate, prepare application form.

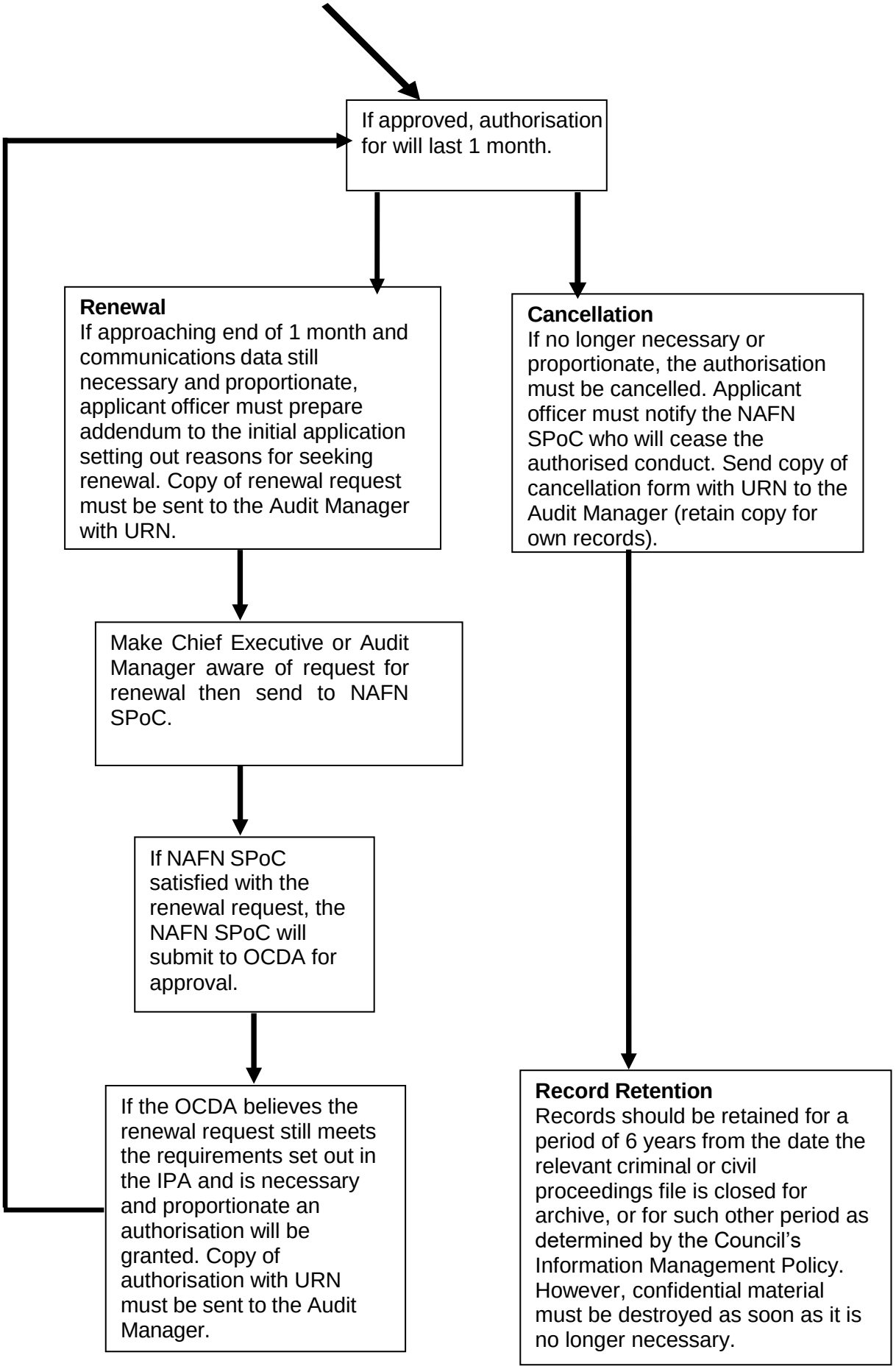
Notify Chief Executive or Audit Manager of application & provide original application form to Audit Manager. Audit Manager will return a copy with a URN (retain copy for own records).

Submit application to SPoCs at NAFN for advice. If NAFN SPoC satisfied with the application the NAFN SPoC will submit to OCDA for approval.

If the OCDA believes the acquisition of communications data meets the requirements set out in the IPA and is necessary and proportionate an authorisation will be granted. Copy of authorisation with URN must be sent to the Audit Manager.

If request is refused by the OCDA options are:
•not to proceed;
•resubmit the application with a revised justification and/or a revised course of conduct to acquire communications data; or
•resubmit the application with the same justification and same course of conduct seeking a review of the decision by the OCDA.

Copy of refusal with URN must be sent to the Audit Manager.


If approved, authorisation for will last 1 month.
Renewal
If approaching end of 1 month and communications data still necessary and proportionate, applicant officer must prepare addendum to the initial application setting out reasons for seeking renewal. Copy of renewal request must be sent to the Audit Manager with URN.
Cancellation
If no longer necessary or proportionate, the authorisation must be cancelled. Applicant officer must notify the NAFN SPoC who will cease the authorised conduct. Send copy of cancellation form with URN to the Audit Manager (retain copy for own records).
Make Chief Executive or Audit Manager aware of request for renewal then send to NAFN SPoC.
If NAFN SPoC satisfied with the renewal request, the NAFN SPoC will submit to OCDA for approval.
If the OCDA believes the renewal request still meets the requirements set out in the IPA and is necessary and proportionate an authorisation will be granted. Copy of authorisation with URN must be sent to the Audit Manager.
Record Retention
Records should be retained for a period of 6 years from the date the relevant criminal or civil proceedings file is closed for archive, or for such other period as determined by the Council's Information Management Policy. However, confidential material must be destroyed as soon as it is no longer necessary.

This page is intentionally left blank

RISK MANAGEMENT POLICY

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

Version 6

July 2023

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

RISK MANAGEMENT POLICY

1. INTRODUCTION

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

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

2. RISK MANAGEMENT STRUCTURE

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

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

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

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

3. AIMS OF THE POLICY

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

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

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

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

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

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

4. RISK MANAGEMENT POLICY

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

(a) <u>Identification / Consideration of Risks</u>

- 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 forlikelihood and impact, identify mitigating controls and allocate responsibility for themitigating controls.

(b) Development Delivery

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

(c) Member Involvement / Responsibility

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

(d) Training / Awareness

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

(e) Review

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

(f) Business Continuity

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

(g) Insurance

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

(h) Controlling the Risks

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

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

5. RISK APPETITE

5.1 The Council's risk appetite guides how much risk it is willing to seek or accept to achieve its objectives. The Council recognisse that it will need to take risks, both in ordinary business and to achieve the priorities set out in the Council Delivery Plan. Good risk management ensures well informed decisions are made, and the associated risks are understood. By ensuring that risks are properly responded to, the Council will be more likely to achieve its priorities. It also provides control and a high level of due diligence consistent with the Council's responsibilities in managing public money.

5.2 The Council recognises effective risk management considers not just threats but also opportunities. So, the Council's approach to risk is to seek the right opportunities and, where possible, minimise threats. By encouraging managed risk taking and considering all of the available options the Council seeks a balance between caution and innovation.

5.3 The Council's risk appetite reflects the current position; encouraging managed risk taking for minor to moderate level risks but controlling more closely those risks that come further up the scale. The appetite for risk will vary over time depending on ambitions and priorities and the operating environment.. Resources are aligned to priorities and arrangements are in place to monitor and mitigate risks to acceptable levels.

5.4 Beyond the Counci's risk appetite is its risk tolerance. This sets the level of risk that is unacceptable, whatever opportunities might follow. In such instances the Council will aim to reduce the risk to a level that is within its appetite. Whilst appetite may be lower, tolerance levels may be higher, and the Council recognises that it is not possible or necessarily desirable to eliminate some of the risks inherent in its activities. In some instances, acceptance of risk within the public sector is necessary due to the nature of services, constraints within operating environment and a limited ability to

directly influence where risks are shared across sectors.

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

6. CORPORATE RISK SCRUTINY GROUP

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

6.2 The role of the Group is to maintain a formal framework that will assist with the management of risk and business continuity, by developing the corporate lead and advising CLT on the expected outcome. The objectives of the Group are:

- to assess and advise on the reduction of prevailing risks within the Council's services, to the benefit of staff and the public;
- to discuss, agree and recommend as appropriate, on matters relating to corporate risk policy;
- to make reports and recommendations to CLT;
- to discuss operational risks insofar as they relate to matters of cross-directorate interest;
- to oversee the implementation of the Council's Risk Management Policy, and topromote a holistic approach to its ongoing management;
- to promote good risk management practices with the aim of reducing potential liabilities;
- to consider and identify new risks, and ideas / schemes for risk reduction;
- to provide a forum to discussion on risk management issues.

These will be achieved through the following:

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

occurrence;
- supporting the review of the risk register and action plans to ensure that appropriate management action is taken appropriately to tolerate, treat, transfer or terminate the risk;
- monitoring compliance with legal and statutory duties;
- providing progress reports to CLT and members, drawing to their attention significant business risks;
- encouraging localised Risk Registers to be created where necessary, as well as supporting dynamic risk assessment.

7. PROCEDURES

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

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

8. FUNDING FOR RISK MANAGEMENT

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

9. BENEFITS OF EFFECTIVE RISK MANAGEMENT

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

<u>Improved Strategic Management</u>

- 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

<u>Improved Operational Managements</u>

- 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

<u>Improved Financial Management</u>

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

Improved Customer Service

- Minimal service disruption to customers and a positive external image

10. CURRENT CHALLENGES FACING THE COUNCIL

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

- Providing services through the cost of living crisis. This impacts on the Council from a cost pressure perspective as its cost base is increasing and from a service delivery perspective as there is greater demand for the services provided by the Council.
- Ensuring financial sustainability over the medium term.
- Embedding the new Council following the District elections in May 2023.
- Ensuring our business continuity and information technology security arrangements futureproof.
- Working with partners to establishing the East Midlands Freeport
- Keeping abreast of Government policy changes, for example the requirements of the recently created Office for Local Government.
- Continually developing our compliance and assurance frameworks to ensure robust decision making.
- Meeting the net zero commitment to be carbon neutral as a Council by 203 and as a district by 2050.

APPENDIX A

RISK MANAGEMENT FRAMEWORK

(A) What is the framework?

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

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

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

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

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

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

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

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

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

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

(C) Assessing risk

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

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

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

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

Table 1 - assessing the likelihood of exposure

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

Table 2 - assessing the impact of exposure

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

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

(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 Council's 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													
	Risk Description	Consequence	Cause	Inherent Risk			Responsibility of	Responsible to	Control Measures	Residual Risk			
Ref No.				Impact	Likelihood	Rating				Impact	Likelihood	Rating	Movement of Risk

(F) Roles of Officers

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

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

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

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

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

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

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

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

This page is intentionally left blank

NORTH WEST LEICESTERSHIRE DISTRICT COUNCIL
CABINET – TUESDAY, 19 SEPTEMBER 2023

Title of Report	**DRAFT 2023/24 QUARTER 1 GENERAL FUND AND HOUSING REVENUE ACCOUNT (HRA) FINANCE UPDATE**	
Presented by	Councillor Nick Rushton Corporate Portfolio Holder PH Briefed [X]	
Background Papers	**Cabinet 31 January 2023:** General Fund Budget & Council Tax 2023/24 HRA Budget & Rents 2023/24 Capital Strategy, Treasury Management Strategy & Prudential Indicators 2023/24 Corporate Scrutiny Committee Minutes – 31 August 2023	**Public Report:** Yes **Key Decision:** Yes
Financial Implications	Any financial implications of this report are detailed in the body of the report and the attached appendices.	
	Signed off by the Section 151 Officer: Yes	
Legal Implications	No legal implications arising from this report.	
	Signed off by the Monitoring Officer: Yes	
Staffing and Corporate Implications	Any staffing implications of this report are detailed in the body of the report and the attached appendices.	
	Signed off by the Head of Paid Service: Yes	
Purpose of Report	To provide Cabinet with an update on the financial position on the General Fund and Housing Revenue Account (HRA) as at Quarter 1 2023/24.	
Reason for Decision	To update Cabinet on Quarter 1 and request approval for supplementary estimates as detailed in the recommendations below.	
Recommendations	**CABINET IS RECOMMENDED TO:** **1. NOTE THE FORECAST OVERSPEND ON GENERAL FUND FOR 2023/24 OF £252K BASED ON QUARTER 1**	

	INFORMATION. **2. NOTE THE SPECIAL EXPENSES FORECAST OUTTURN FIGURES FOR 2023/24 BASED ON QUARTER 1 INFORMATION.** **3. NOTE THE FORECAST OVERSPEND ON THE HOUSING REVENUE ACCOUNT FOR 2023/24 OF £436K BASED ON QUARTER 1 INFORMATION.** **4. NOTE THE SUPPLEMENTARY ESTIMATES DETAILED ON APPENDIX 2(c) WHICH ARE BELOW £100K AND ARE EXTERNALLY FUNDED.** **5. APPROVE THE SUPPLEMENTARY ESTIMATES DETAILED ON APPENDIX 2(c) WHICH ARE ABOVE £100K AND ARE EXTERNALLY FUNDED.** **6. APPROVE ALL SUPPLEMENTARY ESTIMATES DETAILED ON APPENDIX 2(c) WHICH REQUIRE COUNCIL FUNDING.** **7. NOTE THAT THE SUPPLEMENTARY ESTIMATES DETAILED ON APPENDIX 2(c) WHICH ARE ABOVE £250K AND ARE EXTERNALLY FUNDED, WERE APPROVED BY FULL COUNCIL ON 5 SEPTEMBER 2023.** **8. NOTE THE REVISED 2023/24 GENERAL FUND CAPITAL PROGRAMME BUDGET DETAILED IN APPENDIX 5 AS APPROVED BY FULL COUNCIL ON 5 SEPTEMBER 2023.** **9. NOTE THE REVISED HOUSING REVENUE ACCOUNT CAPITAL PROGRAMME DETAILED IN APPENDIX 9.**

1.0 PURPOSE OF THE REPORT

1.1 To inform Members of the spending position for the period 1 April 2023 to 30 June 2023 for the Council's General Fund, and Housing Revenue Account (HRA), and update them of any significant variances from the approved budgets.

1.2 To update Members on supplementary estimates requested and to request approval for those over £100k which are externally funded and for approval for any which are Council funded.

1.3 To update Members on the capital programme for the period 1 April 2023 to 30 June 2023 on the proposed resourcing of the capital programme and the level of Council capital resources available, including capital receipts.

1.4 To update Members on the changes to the capital programme and note the variations to scheme budgets and re-profiling of budgets to future years.

1.5 To provide Members with an update on the Council's Treasury Management activity during the period 1 April 2023 to 30 June 2023.

2.0 GENERAL FUND

2.1 General Fund Revenue

2.1.1 Table 1 below summarises the first quarter position summarised by Directorates. The current projections are that an overspend of £252k on the overall General Fund budget is expected to occur for 2023/24.

Table 1 – General Fund Revenue 2023/24 Quarter 1 Forecast Outturn Position

Directorate	Annual Budget	Forecast Outturn	Forecast Outturn Variance
	£'000	**£'000**	**£'000**
Chief Executive Directorate	2,797	2,797	0
Place Directorate	2,478	2,596	118
Communities Directorate	8,078	8,046	(32)
Resources Directorate	3,488	3,503	15
Corporate and Democratic Core and Other Budgets	896	1,344	448
NET COST OF SERVICES	**17,737**	**18,286**	**549**
Net Recharges from General Fund	(1,828)	(1,828)	0
NET COST OF SERVICES AFTER RECHARGES	**15,909**	**16,458**	**549**
Corporate Items and Financing	1,444	1,171	(273)
NET REVENUE EXPENDITURE	**17,353**	**17,629**	**276**
Contribution to/(from) Balances/Reserves	(266)	(290)	(24)
NET EXPENDITURE (AFTER RESERVE CONTRIBUTIONS)	**17,087**	**17,339**	**252**

2.1.2 Cabinet should note that the estimated overspend at quarter one is a forecast only and may reduce or increase. Close monitoring of performance against budget must be a top priority for managers to identify any areas that pose significant budget pressures.

2.1.3 There are a number of variances that make up the forecast outturn detailed above. Appendix 1 gives a more detailed analysis of the forecast outturn variances by service area. A summarised analysis of the major factors are detailed below along with mitigating factors which service areas have identified to offset some of these areas of overspending:-

Place Directorate £118k

- Property £33k – the forecast overspend is largely due to a significant leak in the roof at the Courtyard development which has required emergency works at a cost of circa £30k. Some of this should be claimed back from the insurers but the amount is unknown at the moment.
- Planning £85k – this is largely due to a forecast overspend of £75k on additional agency costs and £10k for other staffing costs. The Planning Service has been advised that two major and strategic applications for residential and employment development are expected to be submitted in Quarter 4 and if both applications are submitted the fee income received would likely be between £450-600k. There a risk the fee income may not be received until the 2024/25 financial year.

Community Services Directorate

- New Market £30k – there is currently a forecast shortfall in income due to the loss of traders although other traders have been approached and are interested in growing their business.

- Leisure Services £63k – As part of the leisure contract the contractor can claim additional funding to cover significant increases in the price and cost of electricity and gas, subject to a utility benchmarking exercise being undertaken. Any amount claimed in 2023/24 will depend on utility prices and the profitability of the leisure centres during the year. The forecast is based on a provisional figure for 2022/23 which is still to be confirmed and is subject to negotiation.

- Waste Services – there is likely to be increased recycling income if prices and tonnages remain at current levels along with increased trade refuse income if the current number of customers are retained and green bin income is on budget. This additional income will be offset by increased vehicle hire costs due to delayed delivery of refuse vehicles due to worldwide market shortages and delays on parts and raw materials and increased agency staff to cover sickness and absence levels. As a result of the uncertainty around these figures the forecast on Waste Services remains on budget, however, further work is being undertaken ahead of the quarter two reporting.

- Strategic Housing (£125k) – Housing is utilising external grant income received for the Rough Sleeping Initiative and Ukraine specific Homelessness Prevention Grant to fund expenditure already included within the revenue budget leading to this saving.

Corporate, Financing and Other Budgets

- Pay award £448k – the Council has included 4% in the 2023/24 budget for the pay award, but the latest indications are that this could be as high as 6.75%. Final confirmation of the actual pay award is still to be received. Part of the pay award for Chief Officers has been agreed at 3.5% which is under forecast.

- Investment Income (£273k) – this increase is largely due to the further increases in interest rates by the Bank of England. Additionally, investment balances have been higher than expected due to a number of factors including delayed repayment of grants to central government, increased level of reserves,

slippage in capital programmes and extended periods between receipts and payments.

2.1.4 There continues to be pressures within the Finance Team budget due to the continued delays in the production and audit of the Council's 2021/22 and 2022/23 Statement of Accounts. The Team is also experiencing issues with the recruitment and retention of key positions. These are currently being filled using interim support and are essential as the process for setting the 2024/25 budget commences. All additional costs will be offset against the increase in income from treasury management activities.

2.1.5 Although the forecast outturn detailed above is showing a £252k overspend, services are working to mitigate these areas of overspending, as detailed in the bullet points in paragraph 2.1.3 above, along with the potential of increased Planning fee income which would mitigate against the current overspend position.

2.1.6 Managers are expected to bring their spending back within budget which the Council successfully achieved in the last financial year. The implications on the Medium Term Financial Plan (MTFP) also need to be considered as there is a substantial gap to be closed. There is a budget shortfall in 2024/25 of £1.6m which rises to an annual budget shortfall of £3.9m in 2027/28. This is a cumulative gap over the course of the five-year MTFP of £10.2m.

2.1.7 Officers are also exploring options for any potential funding opportunities available. An example of this is the Planning Skills Delivery Fund (PSDF) recently launched by the Department of Levelling Up, Housing and Communities (DLUHC). Local Planning Authorities can now apply for funding (up to £100k), which can be used to hire additional planning officers and invest in other resources to help clear planning backlogs. Officers are assessing whether the Council meets the bidding criteria and if the Council is eligible, a bid will be submitted. There are, however, no guarantees that the Council would be successful.

2.2 Virements

2.2.1 A virement is where one or more budget(s) are reduced to fund an increase in another budget(s). There is no net change in the total budget agreed by Council arising from a virement.

2.2.2 New virement approval levels were approved as part of the constitution by Council in February 2023. These approval levels are detailed in Appendix 2(a).

2.2.3 There are no virements within quarter one which require approval by either Cabinet or Council.

2.3 Supplementary Estimates

2.3.1 Supplementary estimates are a new process that was also approved as part of the constitution by Council in February 2023 as per paragraph 2.2.2 above. These approval levels are detailed in Appendix 2(b).

2.3.2 A supplementary estimate is an addition to the Council's agreed budget and should only be considered after all other options such as virements or savings have been considered.

2.3.3 Supplementary estimates include budgets fully funded by external grants or contributions.

2.3.4 All supplementary estimates which require Council funding require Cabinet approval whereas those fully externally funded are reported to Cabinet below £100k but require approval over £100k.

2.3.5 Appendix 2(c) details all supplementary estimates grouped by value and funding with details of the reasons for the requests. As can be seen from Appendix 2(c), the total external funding to be included in the 2023/24 budgets is £1.87m (of which £123k is capital) and the total to be transferred from reserves is £197k (of which £120k is HRA).

2.4 Section 106

2.4.1 Section 106 funds of £7.4m were held by the Council as at 31 March 2023. These funds will be spent by several organisations including the Council but also parish councils, health authorities etc. A breakdown of the £7.4m is provided at Appendix 3.

2.4.2 Future quarterly reports will be developed throughout the year to provide further detailed information to members on the status of monies spent or held through S106 agreements and their expiry date where relevant.

2.4.3 For information, the figure provided on the reserves balance for S106 in Table 2 will not reconcile to any figures in Appendix 3. This is because the S106 balances are made up of amounts which have already been spent against and are accounted for as a Council reserve, as well as amounts held with no expenditure against them which are accounted for as a liability as they could potentially be returned to the payer.

2.5 General Fund Reserves

2.5.1 The Council holds reserves that are earmarked for a particular purpose and are set aside to meet known or predicted future expenditure in relation to that purpose. The reserves are monitored alongside the budget as part of budget monitoring.

2.5.2 Assuming that reserves are utilised in line with the timescales agreed as part of their approval, reserves represent an effective means of utilising surpluses and underspends and ensuring delivery of projects.

2.5.3 Best practice indicates that reserves, if set aside for specific purposes should be spent in accordance with projections. Finance clinics (this is a dedicated meeting between finance officers and Heads of Service/Team Managers) focus on ensuring that earmarked reserves are expended in a timely manner in line with the purposes in which they have been set aside.

2.5.4 Table 2 below summarises the forecasted position in respect of earmarked reserves and other reserves held by the Council. Full details by service can be found in Appendix 4.

Table 2 – Usable Reserves forecast at 31 March 2024

Reserves	Balance at 01/04/2023 £m	Forecast Spend £m	No longer required £m	Forecast balance at 31/03/2024 £m
General Fund				
General Fund Earmarked Reserves	6.042	(1.867)	(0.122)	4.053
General Fund General Reserves (agreed minimum balance)	1.544			1.544
Medium Term Financial Plan (MTFP) Reserve	7.937	(0.383)	0.122	7.676
	15.523	(2.25)	0	13.273
Other				
S106 *	1.968			1.968
	17.491	**(2.25)**	**0**	**15.241**

* Balance at 01/04/22, please also see paragraph 2.4.3 above

2.5 General Fund Capital

2.5.1 Table 3 below details the quarter one position on the 2023/24 capital programme. Spend in the period was £0.48m and this was largely by the accommodation programme (work on the Council offices). Full scheme-by-scheme analysis can be found in Appendix 5.

Table 3 - Quarter 1 2023-24 Outturn on the General Fund Capital Programme

Department	Original Budget	Prior Year C/fwd	In-year Changes	Revised Budget	Spend @ P3	23/24 Forecast Outturn	Variance (Rev Budget v Forecast Outturn)	Carry-Forward to Future Years
	£'000	£'000	£'000	£'000	£'000	£'000	£'000	£'000
Place	2,868	8,076	(5,144)	5,800	427	5,159	641	5,080
Community Services	3,597	5,093	(6,510)	2,180	51	2,134	46	6,599
Resource	158	374		532	2	532	0	0
Total	**6,623**	**13,543**	**(11,654)**	**8,512**	**480**	**7,825**	**687**	**11,679**

2.5.2 Expenditure is expected to pick up during the year and the forecast outturn for 2023/24 is £7.8m. £11.6m of the budget is projected to be carried forward to future years. This is detailed in Table 4 below.

Table 4 - Reprofiling of budgets to future years

Department	Reprofiled to 24/25	Reprofiled to 25/26	Reprofiled to 25/26	Total
	£'000	£'000	£'000	£'000
Place	3,878	1,203	0	5,081
Community Services	6,548	0	0	6,598
Resource	0	0	0	0
Total	**10,476**	**1,203**	**0**	**11,679**

2.5.3 Community services has the largest budget allocation to future years and this is mostly due to long lead times in sourcing appropriate environmentally friendly vehicles for the Council's fleet replacement programme. It should be noted the table shows the re-profiling of expenditure from the Budget agreed in February 2023, the majority of the reprofiling was reported to Cabinet as part of the Outturn Report 2022/23. It is being reported again for completeness and transparency. This was also approved by Full Council on 5 September 2023.

2.6 Changes to the Capital Programme

2.6.1 Schemes in the capital programme are grouped under two categories and these are:

Development Pool: These are schemes not yet fully costed or funding sources identified. A full business case is required to be prepared and presented to the newly implemented Capital Strategy Group for consideration before the scheme can go ahead.

Active Programme: Schemes in this category have been approved (by either Capital Strategy Group, Cabinet or Council), fully funded and are being delivered.

2.6.2 Table 5 below details schemes which have moved from the development pool to the active pool during the year.

Table 5 – Scheme Movements in the Capital Programme

Capital Scheme	Revised Budget	Reason for Movement
	£'000	
Schemes Moved to Active Programme		
SharePoint Intranet Upgrade	10	Considered and transferred from development programme to active programme.
Cloud Back-Up Solution	44	Considered and transferred from development programme to active programme.
Laptop Replacement	68	Considered and transferred from development programme to active programme.
Server & Storage Additional Capacity	43	Considered and transferred from development programme to active programme.
CCTV Replacement Programme	95	Considered and transferred from development programme to active programme.
Total Transferred to Active Programme	**260**	
New Schemes Approved by Full Council		
Hermitage Access Road	25	New scheme – funded from existing scheme within the development pool
EcoPark	162	New scheme - externally funded via grant receipts.

Capital Scheme	Revised Budget	Reason for Movement
Public Conveniences	23	New scheme - Funded from underspends within the programme.
Total New Schemes Approved	**210**	

2.6.3 As detailed in Table 5, there are three new schemes added to the Capital Programme that were approved by Council on the 5 September:

Ecopark (Total cost £162k, funded £130k UKSPF grant monies and £32k external contribution from National Forest) At its meeting on 25 July 2023 Cabinet approved a report in relation to the Hermitage Recreation Ground EcoPark. This report included the creation of a new scheme for inclusion in the Council's Capital Programme. The total cost of this scheme is £162k. The scheme is to be funded by a £130k virement from grant monies received from the UK Shared Prosperity Fund (UKSPF) and an external contribution of £32.26k from the National Forest.

Hermitage Access Road Enabling Works (Total cost £25k, funded by virement from underspend on Hermitage Leisure Centre Demolition) The redevelopment of the former Hermitage Leisure Centre site for new uses will require the provision of a new access road designed and constructed to adoptable standard. This scheme proposes the cost of preparing designs and cost estimates for the road and generally progressing preparatory works to the point at which a planning application (for the road) can be submitted. It should be noted if for any reason the scheme did not progress these costs would need to be funded from revenue.

Public Conveniences (Total cost £23k, funded by virement from underspend on IT Programme) Installation of cashless electronic payment facilities at the Council's public toilet facilities as part of the implementation of an invest to save proposal agreed as part of the Budget approved by Council in February 2023. This will enable the Council to achieve the income budget of £16,000. It will also have the potential to lead to further revenue savings in relation to cleaning costs in future years.

2.6.4 One of the major schemes in the capital programme is the Accommodation Project. This scheme is the major refurbishment of the Council offices which includes works to the new customer service centre, Whitwick Business Centre and Stenson House. The total scheme budget is £5.01m and the current forecast spend is £5.43m. This means the scheme is anticipated to overspend by £0.42m. The overspend is due to inflation and the need to undertake backlog strategic maintenance works especially to Stenson House. Undertaking the backlog maintenance works now has prevented additional expenditure in the future. The overspend will be financed from the capital programme contingency fund and re-purposing from existing property strategic maintenance budgets.

3.0 SPECIAL EXPENSES

3.1 Table 6 below summarises the forecast outturn position for Coalville Special Expenses and Other Special Expense areas. Further information is contained within Appendix 6 which provides a more detailed analysis.

3.2 At the end of the first quarter, actual expenditure, including grounds maintenance, events and burial income are all forecast to be on budget.

3.3 The total Special Expenses net revenue budget for 2023/24 is £591k which is funded through Council Tax and Grants of £602k which provides a budgeted surplus of £11k to be transferred to reserves.

Table 6 - Special Expenses 2023/24 Q1 Monitoring & Forecast Outturn Position

SPECIAL EXPENSES	Approved Budget	Forecast Outturn	Variance
	£'000	£'000	£'000
Annual Recurring Expenditure	591	591	0
Expenditure Requirement	591	591	0
Precept	586	586	0
Localisation of Council Tax Support Grant	16	16	0
Transfer from/(to) reserves	(11)	(11)	0

3.4 The provisional balances as at 1 April 2023 and the forecast outturn as at 31 March 2024 are shown in table 7 below. As can be seen from the table, two of the Special Expense areas are forecast to be in a deficit position. This is not a sustainable position and further work is planned for 2023/24, including a review of the Special Expenses Policy, to ensure that a minimum of 10% balances are retained.

Table 7 - Forecasted Special Expense Balances 2023/24

Special Expense Balances	Provisional Balances 01.04.23	Forecasted Contribution to/(from) Balances	Forecasted Balances 31.03.24 Surplus/ (Deficit)
	£	£	£
Coalville	19,150	(2,402)	16,748
Whitwick	7,664	6	7,670
Hugglescote/Donington Le Heath	17,851	5,717	23,568
Coleorton	1,274	1,650	2,924
Lockington/Hemington	1,272	886	2,158
Measham	1,107	695	1,802
Oakthorpe & Donisthorpe	(17,250)	1,373	(15,877)
Ravenstone	492	887	1,379
Stretton	(1,501)	1	(1,500)
Appleby Magna	844	1,650	2,494

SPECIAL EXPENSE BALANCES	Provisional Balances 01.04.23	Forecast Contribution to/(from) Balances	Forecast Balances 31.03.24 Surplus/ (Deficit)
	£	£	£
Coalville	19,150	(2,402)	16,748
Whitwick	7,664	6	7,670
Hugglescote/Donington Le Heath	17,851	5,717	23,568
Coleorton	1,274	1,650	2,924
Lockington/Hemington	1,272	886	2,158
Measham	1,107	695	1,802
Ravenstone	492	887	1,379
Appleby Magna	844	1,650	2,494

3.5 A list of the Special expense earmarked reserves as at the end of June 2023 are shown in table 8 below. Appendix 7 gives a more detailed analysis.

Table 8 - 2023/24 Special Expenses Earmarked Reserves

EARMARKED RESERVES	Balances 01.04.23	Spend to date	Forecast Spend	Forecast Balance as at 31.03.24
	£	£	£	£
Coalville	92,998	3,974	92,998	0
Hugglescote	28,720	0	28,720	0
Whitwick	9,088	0	9,088	0
	130,806	**3,974**	**130,806**	**0**

4.0 HOUSING REVENUE ACCOUNT (HRA)

4.1 HRA Income and Expenditure

4.1.1 Table 9 below shows the summary income and expenditure forecast outturn and variance for the HRA which is currently forecasting an overspend position at the end of quarter one of £436k.

Table 9 – HRA 2023/24 Quarter 1 Forecast Outturn Position

	Budget £'000	Forecast £'000	Variance £'000
Income	(20,139)	(20,183)	(44)
Operating Expenditure	17,077	17,556	480
Operating (surplus)/deficit	**(3,062)**	**(2,627)**	**436**
Appropriations	7,541	7,541	0
Net (surplus)/deficit	**4,479**	**4,914**	**436**

4.1.2 The service will seek to recover the budget position through vacancy management and use of reserves. A more detailed table can be found at Appendix 8.

4.1.3 The Council is actively working to improve services delivered by the HRA and ensure the impact on tenants is considered in all service delivery. Work on this so far has included:

- Commissioning an independent review of processes.
- Use of contractors to assist in delivering against repairs backlogs.
- Working on reconfiguration of IT systems to improve efficiency and facilitate improved processes.
- Recruiting staff to key vacant roles.
- A plan for further actions within the service is also under preparation.

4.1.4 To address these improvements, it is proposed to utilise £121k of HRA reserves. The approvals for these are being sought as part of the Supplementary Estimates set out in Appendix 2.

4.1.5 Other variances include:

- £180k anticipated shortfall for 2023/24 pay award. The Council has included 4% in the 2023/24 budget for the pay award, but latest indications are that this could be as high as 6.75%. Final confirmation of the actual pay award is still to be received.
- Improvement in expected investment income of £119k due to higher interest rates.
- £75k adverse variance for rent income based on first quarter rents received.

4.1.6 The overspend of £436k will reduce by £121k if the reserve drawn downs detailed in Appendix 2 are approved.

4.2 HRA Reserves

4.2.1 The HRA currently has a balance of £7.2m. A minimum balance of £1.0m is maintained to ensure the HRA has sufficient funding to cover unforeseen revenue expenditure and the remaining £6.2m to be used for capital projects and for the repayment of debt.

4.2.2 Earmarked reserves were reviewed in 2022-23 and as a result, all earmarked reserves were transferred to a Medium Term Financial Planning reserve for the HRA. This will enable reserves to be allocated corporately to achieve strategic aims.

4.2.3 Table 10 below shows a summary of usable HRA reserves:

Table 10 – HRA Usable Reserves forecast 2023/24

Reserves	Balance at 31/03/23 £m	Forecast Contributions Received £m	Forecast Spend Required £m	Balance at 31/03/24 £m
Housing Revenue Account				
HRA Medium Term Financial Plan Reserve	0.53			0.53
HRA Balance	7.20		(4.92)	2.28
	7.73	0.00	(4.92)	2.81
HRA Capital Receipts	11.34	2.76	(6.51)	7.59
Major Repairs Reserve	2.73	3.40	(3.47)	2.66
Debt Repayment Reserve	0.00	3.73	0.00	3.73
	21.80	**9.89**	**(14.90)**	**16.79**

4.3 HOUSING REVENUE ACCOUNT CAPITAL PROGRAMME

4.3.1 The Housing capital programme broadly consists of the Improvements and Modernisation programme as well as the New Build programme.

4.3.2 The Improvements and Modernisation Programme includes:

- Vital fire safety works.
- Major aids and adaptation works around safety, accessibility and increasing independent living for residents.
- Transforming older persons schemes to an integrated digital service, giving full and timely works and events and visits information to residents. This also allows the Council to share a digital layout with the Fire Service so in the event of an incident they can guide crews through the building.
- Replacement heating scheme, installing new Ideal Logic (hydrogen ready) efficient boilers or air source heat pumps (if replacing solid fuel systems) and correct insulation to improve thermal efficiency of Council homes. This will improve affordability of heating for tenants this winter as well as assisting the Council in achieving progress towards every property meeting Energy Performance Certificate Level C by 2028.

4.3.3 Most of the projects in the new build scheme are still at the design stage. The Council is exploring a number of delivery models to increase the number of affordable and social housing units across the District.

4.3.4 Table 11 shows the expenditure and forecast against budget as at quarter one.

Table 11 - Quarter 1 2023/2024 Outturn on the HRA Capital Programme

Scheme	Original Budget	Prior Year C/fwd	In-year Changes	Revised Budget	Spend @ P3	23/24 Forecast Outturn	Variance (Rev Budget v Forecast Outturn)	Carry-Forward to Future Years
	£'000	£'000	£'000	£'000	£'000		£'000	£'000
Improvements & Modernisation	12,226	8,555	(8,486)	12,295	1,286	12,045	250	7,612
New Build	2,948	6,148	(7,078)	2,018	5	2,018	0	7,857
Total	**15,174**	**14,703**	**(15,564)**	**14,313**	**1,291**	**14,063**	**250**	**15,469**

4.3.5 Expenditure for quarter one was £1.29m and this was largely from the improvements and modernisation programme. This low level of expenditure for quarter one is the result of taking an early review of the programme in the context of sector wide issues as well as the time take to procure contractors.

4.3.6 The forecast is £0.25m below budget. This is mainly on the Homes Improvement Programme where the expenditure of £4.3m is forecast against a budget of £4.5m. This is the result of the programme of expenditure being allocated against workstreams with realistic timings. The programme will be continued to be monitored against these timings.

Table 12 - Reprofiling of Future Years Budgets

Scheme	Reprofiled to 24/25	Reprofiled to 25/26	Reprofiled to 25/26	Total
	£'000	£'000	£'000	£'000
Improvements and Modernisation	2,793	5	5,738	8,536
New Build	1,139	0	5,794	6,933
Total	**3,932**	**5**	**11,532**	**15,469**

4.3.3 The improvements and modernisation programme has the largest budget allocation to future years and this is to undertake projects such as fire safety works, roof replacement and zero-carbon schemes.

4.3.4 It should be noted the table shows the re-profiling of expenditure from the Budget agreed in February 2023, the majority of the reprofiling was reported to Cabinet as part of the Outturn Report 2022/23. It is being reported again for completeness and transparency but is expected to be refined again at the end of Quarter 2.

4.3.5 Changes to the QL Housing and Repairs data system mean the Council will be recording in more detail and in real-time what budgets are being spent, when, and where. This system is in the process of being integrated with the Unit4 Finance system so that weekly reconciliation of forecast and actual budgets can be undertaken. Where programmes fall behind in delivery, adjustments can be made to ensure the Council delivers what it promise or communicates and takes action to intervene.

5.0 TREASURY MANAGEMENT

5.0.1 The following outlines the Treasury position and variance to budget of the Council's Treasury management function. The Council's treasury management strategy for 2023/24 was approved at a Council meeting on 23 February 2023. The Council has invested substantial sums of money and is, therefore, exposed to financial risks

including the loss of invested funds and the revenue effect of changing interest rates. The successful identification, monitoring and control of risk remains central to the Council's treasury management strategy.

5.0.2 Table 13 shows the progression of budgets as at 30 June 2023 for Treasury Management elements.

Table 13 – Treasury Management Forecast Outturn 2023/24

Element	Original Budget	Variance	Revised Forecast
	£'000	**£'000**	**£'000**
Investment Interest Income:			
Deductions	(189)	(104)	(293)
GF	(336)	(273)	(609)
HRA	(457)	(119)	(576)
Total	**(982)**	**(496)**	**(1,478)**
Borrowing Interest Expenditure	2,228	0	2,228
Borrowing Principle Repaid	2,734	0	2,734
Total	**3,980**	**(496)**	**3,484**

5.0.3 Table 14 shows a summary of the Council's external investments and borrowing along with the rate of return/borrowing of both. The movements from 31 March 2023 are shown in Table 15 below:

Table 14 – Treasury Summary

	31.3.23 Balance £m	Movement £m	30.06.23 Balance £m	30.06.23 Rate %
Long-term borrowing	59.8	0.0	59.8	3.6%
Short-term borrowing	2.7	0.0	2.7	4.2%
Total borrowing	**62.5**	**0.0**	**62.5**	**3.6%**
Long-term investments	0.0	0.0	0.0	0.0%
Short-term investments	39.0	(4.0)	35.0	4.6%
Cash and cash equivalents	4.1	13.9	18.0	4.7%
Total investments	**43.1**	**9.9**	**53.0**	**4.7%**
Net borrowing	**19.5**	**(9.9)**	**9.6**	

5.0.4 Further information on the Council's borrowing and investments can be found on Appendix 10.

5.0.5 One of the investments held by the Council is a loan of £5m to Birmingham City Council. On 5 September 2023, Birmingham issued a Section 114 notice, stating that they lack the necessary resources to balance their budget. This shortfall primarily arises from their inability to meet sustainable liabilities linked to increasing equal pay claims. It's important to emphasise that the Council's funds are secure, as they are backed by central government support. The Council's treasury advisors at Arlingclose have confirmed this, expressing full confidence that the investments will be repaid in

full at maturity. Previous instances of Section 114 notices at other local authorities have not led to investments going unpaid. The investment itself was £5m, at a 4% interest rate, with a one- year duration. The investment is set to mature on 25 January 2024, having commenced on the 26 January 2023.

Policies and other considerations, as appropriate	
Council Priorities:	The spending from the budget provides funding for the Council to deliver against all its priorities.
Policy Considerations:	None
Safeguarding:	None
Equalities/Diversity:	None
Customer Impact:	None
Economic and Social Impact:	The Council plans to invest up to £3.5m in town centre regeneration and public realm works in the current financial year.
Environment and Climate Change:	The Council plans to invest up to £3.1m retrofitting Council homes to make them carbon neutral. Up to £0.5m is forecast to be spent on purchasing environmentally friendly vehicles and installing electric vehicle charging points throughout the district in the current financial year.
Consultation/Community/Tenant Engagement:	Corporate Scrutiny Committee 31 August 2023
Risks:	High levels of inflation can undermine the Council's financial reserves. As inflation rises, the real purchasing power of the Council's reserves steadily erodes, meaning the same amount of money can purchase progressively fewer goods and services. This erosion of value poses a challenge to the organisation's ability to maintain financial stability and achieve its long-term financial objectives. Furthermore, the Council has opted to allocate its increased interest earnings (resulting from increased base rate) towards funding its base revenue budget rather than reinvesting them into reserves. This strategic choice, combined with the inflationary pressure, leads to an overall devaluation of reserves. Essentially, this practice leaves the organisation with reduced financial resilience, as it does not adequately account for the eroding effect of inflation on its reserves. Although the current high levels of inflation are causing problems, reserves might be expected to

	grow with more moderate levels of inflation over the long term. Real returns (i.e. after inflation) are and have been negative despite investment returns rising. So even if the Council changed its policy to add interest earnings to reserves it still would not solve the whole problem. Indeed, very few investment returns are beating inflation and in general if you wanted higher returns you'd need to invest for a longer period and/or with riskier assets, which the council has decided not to do. The budgets will continue to be monitored throughout the year to ensure the Council remains within its funding envelope.
Officer Contact	Anna Crouch Head of Finance & Deputy S151 Officer anna.crouch@nwleicestershire.gov.uk

This page is intentionally left blank

Appendix 1

2023/2024 GENERAL FUND REVENUE QUARTER 1 FORECAST OUTTURN POSITION

Directorate & Service Area	Annual Budget	Forecast Outturn	Forecast Outturn Variance
	£'000	£'000	£'000
Chief Executive	402	402	0
Human Resources	740	740	0
Legal & Support Services	1,655	1,655	0
Total Chief Executive Directorate	**2,797**	**2,797**	**0**
Strategic Director of Place	341	341	0
Property & Economic Regeneration	1,143	1,176	33
Planning	985	1,070	85
Joint Strategic Planning	9	9	0
Total Place Directorate	**2,478**	**2,596**	**118**
Strategic Director of Community Services			
Community Services	6,322	6,415	93
Strategic Housing	798	673	(125)
Customer Services	958	958	0
Total Communities Directorate	**8,078**	**8,046**	**(32)**
Strategic Director of Resources			
Finance	1,148	1,163	15
Revenues & Benefits	1,131	1,131	0
ICT	1,209	1,209	0
Total Resources	**3,488**	**3,503**	**15**
Corporate & Democratic Core (CDC) & Other Budgets			
Corporate & Democratic Core	70	70	0
Pay award	651	1,099	448
Non Distributed - Revenue Exp on Surplus Assets	108	108	0
Non Distributed - Retirement Benefits	67	67	0
Total CDC & Other Budgets	**896**	**1,344**	**448**
NET COST OF SERVICES	**17,737**	**18,286**	**549**
Net Recharges from General Fund	(1,828)	(1,828)	0
NET COST OF SERVICES AFTER RECHARGES	**15,909**	**16,458**	**549**

2023/2024 GENERAL FUND REVENUE QUARTER 1 FORECAST OUTTURN POSITION

Directorate & Service Area	Annual Budget	Forecast Outturn	Forecast Outturn Variance
Corporate Items & Financing			
Net Financing Costs	1,763	1,763	0
Investment Income	(335)	(608)	(273)
Localisation of CT Support Grant - Parish & Special Expenses	16	16	0
Total Corporate Items & Financing	**1,444**	**1,171**	**(273)**
NET REVENUE EXPENDITURE	**17,353**	**17,629**	**276**
Budget Proposals Funded from Reserves - One-Off	(290)	(290)	0
Contribution to/(from) Balances/Reserves	24	0	(24)
NET EXPENDITURE (AFTER RESERVE CONTRIBUTION	**17,087**	**17,339**	**252**

Virements

- Council policy is that it shall **not exceed the budgets allocated** to each relevant budget head.
- However, it shall be **entitled to vire across budget heads** within such limits as shall be laid down in the Financial Procedure Rules.
- A virement is **defined as where one or more budget(s) are reduced to fund an increase in another budget(s).**
- There is **no net change in the total budget agreed by Council** arising from a virement

	Approval Level Required		
Value	**Within a Budget Head**	**Between Budget Heads in same Directorate**	**Between Directorates**
Between £0 - £4,999	Heads of Service	Heads of Service	Heads of Service
Between £5,000 and £24,999	Heads of Service and Chief Executive/Strategic Directors	Chief Executive/Strategic Directors and Portfolio Holder(s)	Chief Executive/Strategic Directors and Portfolio Holder(s)
Between £25,000 and £99,999	Chief Executive/Strategic Directors and Portfolio Holder(s)	Chief Executive/Strategic Directors and Portfolio Holder(s)	Chief Executive/Strategic Directors and Portfolio Holder(s)
Between £100,000 and £249,999	Cabinet	Cabinet	Cabinet
£250,000 and over	Full Council	Full Council	Full Council

Notes:

1. In all circumstances virements require approval by the S151 Officer.
2. All relevant parties listed above must be in agreement.
3. Virements should not be artificially disaggregated.
4. Virement rules apply to capital and revenue.

North West Leicestershire District Council

This page is intentionally left blank

Supplementary Estimates

- A supplementary estimate is an **addition to the Council's agreed budget**.
- Supplementary estimates can be **one-offs, or recurring**
- In either case, supplementary estimates **should only be considered after all other options**, such as virements, or savings, have been considered
- Supplementary estimates **include budgets fully funded by external grant or contribution**

	Approval Level Required	
Value	**Fully Externally Funded**	**Requires Council Funding**
Between £0 and £99,999	Head of Service and Chief Executive/Strategic Directors [then reported to Cabinet at next meeting]	Cabinet
Between £100,000 and £249,999	Cabinet	Cabinet
£250,000 and over	Full Council	Full Council

Notes:

1. In all circumstances Supplementary Estimates require approval by the S151 Officer.
2. Council funding includes (but is not limited to) revenue budget, reserves, Section 106, capital receipts and borrowing. S151 Officer decision will undertaken an assessment.
3. Supplementary Estimates should not be artificially disaggregated.
4. Supplementary Estimates rules apply to capital and revenue.

North West Leicestershire District Council

This page is intentionally left blank

Draft Supplementary Estimates & Virements - General Fund, HRA & Special Expenses (Capital & Revenue)

Capital/ Revenue	General Fund/ HRA / Special Expenses	Directorate	Service	Service Area	Recurring/ One-Off	Amount £	Funded By	Reason For Request
Externally Funded Between £0 and £99,999								
Capital	General Fund	Communities	Public protection team	Public protection team	One-Off	90,264	DLUHC	DFG capital grant adjustment
Capital	General Fund	Communities	Leisure Services	Leisure Services	One-Off	32,260	National Forest	Eco-Park (at Hermitage recreational ground) new funding
						122,524		
Revenue	General Fund	Communities	Housing	Strategic Housing	One-Off	92,397	DLUHC	Ukraine Homeless Prevention Grant
Revenue	General Fund	Communities	Environmental Protection	Community Service	One-Off	70,744	LCC	DFG/Lightbulb Grant (increase for 23/24)
Revenue	General Fund	Communities	Environmental Health/Border Inspection	Community Service	One-Off	16,994	FSA	(FSA)Food Standards Agency Project for Port Health
Revenue	General Fund	Communities	Community Safety	Community Service	Recurring	34,370	DLUHC	Domestic Abuse Grant
Revenue	General Fund	Communities	Stronger & Safer Communities	Community Service	One-Off	6,555	OPPC	CSP/ Police Crime Commissioner-Community Safety projects
Revenue	General Fund	Resources	Revenues & Benefits	Revenues	One-Off	8,116	DLUHC	Business Rates Retention Scheme
Revenue	General Fund	Resources	Revenues & Benefits	Revenues	One-Off	10,565	DLUHC	New burdens for implementing LCTSS
Revenue	General Fund	Resources	Revenues & Benefits	Benefits	One-Off	9,927	DWP	Various benefits grants to be paid out to CAPITA
Revenue	General Fund	Resources	Revenues & Benefits	Benefits	One-Off	12,231	DWP	Benefits HBA (unsure if needs to be paid to CAPITA)
Revenue	General Fund	Resources	Revenues & Benefits	Benefits	One-Off	96	DWP	Benefits Digital Forms (unsure if needs to be paid to CAPITA)
Revenue	General Fund	Chief Exec	Legal & Support	Democratic Services	One-Off	37,235	DLUHC	Electoral Integrity (Voter ID)
Revenue	General Fund	Chief Exec	Legal & Support	Democratic Services	One-Off	2,125	DLUHC	Electoral Integrity (Implementation of Elections Act 2022)
Revenue	General Fund	Communities	Leisure Services	Leisure Services	One-Off	20,600	National Forest	Eco-Park (at Hermitage recreational ground) new funding
Revenue	General Fund	Communities	Cleansing Services	Waste Services	One-Off	10,000	LCC	Grant to purchase additional litter bins throughout the district
						331,955		
Externally Funded Between £100,000 and £249,999								
Revenue	General Fund	Communities	Housing	Strategic Housing	Recurring	143,649	DLUHC	Homeless Prevention Grant
Revenue	General Fund	Place	Property & Economic Regeneration	Economic Regeneration	One-off	117,272	DLUHC	UK Rural England Prosperity Fund (UKREPF) (approved by Cabinet 25-07-23)
Revenue	General Fund	Resources	Revenues & Benefits	Revenues	One-off	124,315	DLUHC	Local Council Tax Support Scheme
						385,236		
Externally Funded Over £250,000								
Revenue	General Fund	Communities	Housing	Strategic Housing	Recurring	531,860	DLUHC	Rough Sleeping Initiative grant
Revenue	General Fund	Place	Property & Economic Regeneration	Economic Regeneration	One-Off	496,121	DLUHC	UK Shared Prosperity Fund Year 2 (UKSPF)
						1,027,981		
TOTAL EXTERNALLY FUNDED						**1,867,696**		
Council Funded Between £0 and £99,999								
Revenue	General Fund	Communities	Housing	Strategic Housing	One-Off	75,693	Earmarked Reserve	Underspend from 22/23 forms part of 23/24 RSI allocation
Revenue	HRA	Communities	Housing	Dir and Head of Housing	One-Off	45,225	HRA Reserve	Additional finance support to enable HRA transformation
Revenue	HRA	Communities	Housing	Dir and Head of Housing	One-Off	75,000	HRA Reserve	Externally produced Asset Management Plan
Revenue	Special Expenses	Communities	Leisure Services	Leisure Services	One-Off	1,274	Coleorton Special Expense Balances	Removal of play equipment and safety surfacing and to grass over the area at Forresters close.
TOTAL COUNCIL FUNDED						**197,192**		
TOTAL SUPPLEMENTARY ESTIMATES						**2,064,888**		

PLEASE NOTE:
THERE ARE NO VIREMENTS FOR APPROVAL AS PART OF THE QUARTER ONE REPORT

This page is intentionally left blank

Appendix 3

SECTION 106

Legal Agreements under Section 106 of the Town and Country Planning Act secure developer contributions to mitigate the impacts of the development on the local area. The District Council holds funds generated from legal agreements on behalf of the Council and third parties, such as the Healthcare bodies or the National Forest Company. The Council then holds those funds in an interest-bearing account until they are spent by the body responsible for implementing the requirements in the legal agreement which secured them.

The table below summarises the position at 31 March 2023 for the various types of contributions included in agreements.

Type of Contribution	Balance 31 Mar 22 £'000	Received 2022/23 £'000	Spent 2022/23 £'000	Interest Received £'000	Balance 31 Mar 23 £'000
River Mease (available to spend)	(195)	(1)	119	(4)	(81)
River Mease (retained until obligation met)	(15)	(10)	0	0	(25)
Air Quality	(50)	0	0	(1)	(51)
Police	(210)	0	0	(4)	(214)
Recreation/Play Areas/Leisure	(816)	(240)	13	(17)	(1,060)
Affordable Housing	(2,271)	0	0	(45)	(2,316)
Parish Councils	(144)	(442)	223	0	(363)
National Forest	(57)	(65)	0	(1)	(123)
Healthcare	(606)	(22)	246	(7)	(389)
Highways	(2,589)	0	0	(51)	(2,640)
Network Rail	(17)	0	0	(1)	(18)
CCTV	(12)	0	0	0	(12)
Land and open space	(109)	0	15	(2)	(96)
Sence Valley	(10)	0	0	0	(10)
Total	**(7,101)**	**(780)**	**616**	**(133)**	**(7,398)**

By way of explanation, the River Mease monies are split in to two pots. Those in the pot to be retained until the obligation is met, is where payment has been made upon the grant of planning permission, but the requirement was for money to be paid at commencement of development. Therefore, until development commences this money cannot be used. If it was and the development did not start, the applicant would be able to reclaim the money.

It is important to note that these figures are not static as contributions can be spent at any time during the year, once a scheme has been prepared. For example, since April, payments have been made out of the Parish Councils total such that there is no longer anything left in this pot to spend.

Future quarterly reports will be developed throughout the year to provide further detailed information to members on the status of monies spent or held through S106 agreements.

This page is intentionally left blank

North West Leicestershire District Council
Estimated Reserves at 31/3/24

TEAM	Provisional balance as at 1/4/23 £	Contributions from fund/ commitments 23/24 £	No longer required £	Estimated balance as at 31/3/24 £	Comments
Earmarked Reserves:					
Chief Exec	475,610	(70,805)		404,805	£334k Dev Co, unknown date for spend. Remaining £71k to be spent in 24/25 funding Business Change Post
Human Resources	30,000	(30,000)		0	
Legal & Support Services	147,010	(134,937)		12,073	Remaining balance for Audit Apprentice post, but currently vacant.
Property & Economic Regeneration	2,313,362	(353,323)		1,960,040	Assumed Marlborough & Kegworth + other minor reserves spent Q4 25/25
Planning	784,343	(378,045)		406,298	Remaining is Land Charges contingency £287k to utilise future years shortfall, Neighbourhood Plan funding £93k ongoing.
Joint Strategic Planning	91,017	0		91,017	Contingency - no plans to spend. Belongs to all 10 partners.
Community Services	1,142,425	(675,616)		466,809	£310k climate change ongoing, funding of fixed term posts £113k 24/25, Leisure LRS/LSA £44k ongoing.
Strategic Housing	338,786	(75,694)	(42,408)	220,684	Residual grant funding to be applied to expenditure as appropriate.
Customer Services	16,273	(16,273)		0	
Finance	127,268	(127,268)		0	
Revenues & Benefits	151,645	0	(80,000)	71,645	£80k Contingency for ARG grant no longer needed. Remaining is contingency for Customer Service resource for Household Support.
ICT	5,500	(5,500)		0	
Other reserves	50,000			50,000	
MTFP Reserve	7,936,684	(383,000)	122,408	7,676,092	Est £107k required for Capital Accountant. Est deficit for year £276k.
Business Rates Reserve	369,093			369,093	
Total earmarked reserves - General Fund	**13,979,017**	**(2,250,461)**	**(0)**	**11,728,555**	
Total earmarked reserves - Special Expenses	**130,807**	**(130,807)**		**(0)**	
TOTAL EARMARKED RESERVES	**14,109,823**	**(2,381,268)**	**(0)**	**11,728,555**	
Other reserves General Fund:					
General Balance (minimum level of reserves)	1,544,493			1,544,493	
Total other Reserves - General Fund	**1,544,493**	**0**	**0**	**1,544,493**	
Other reserves Special Expenses:					
General Balance	31,668			31,668	
Total other Reserves - Special Expenses	**31,668**	**0**	**0**	**31,668**	
TOTAL ALL RESERVES - GENERAL FUND & SPECIAL EXPENSES	**15,685,984**	**(2,381,268)**	**(0)**	**13,304,715**	

This page is intentionally left blank

North West Leicestershire District Council

Quarter 1 2023/24 General Fund Capital Programme Monitor

Scheme	Original Budget	Prior Year C/fwd	In-year Changes	Revised Budget	Expenditure @ P3	23/24 Forecast Outturn	Variance (Revised Budget v Forecast Outturn)	Carry-Forward to Future Years	Notes
	£'000	£'000	£'000	£'000	£'000	£'000	£'000	£'000	
GENERAL FUND									
Active Programme:									
Disabled Facilities Grant	670	123	90	883	0	883	0	0	
Council Offices Works	720	798	0	1,518	361	1,518	0	0	
Finance System Review		138		138	0	138	0	0	
SharePoint Intranet Upgrade	10			10		10	0		Moved from development pool to active programme
Laptop Replacement	68			68	1	68	0		Moved from development pool to active programme
Server and storage additional capacity	70		(20)	50		50	0		Moved from development pool to active programme
Cloud Back-up Solution	10	13	20	43		43	0		Moved from development pool to active programme
Car Parks	0	86	(2)	84	0	84	0	1	
Leisure Centres	0	1,112	(1,112)	0	0	0	0	1,112	
Electric Vehicle Charging Points	0	248	(85)	163	16	127	36	85	
Marlborough Square Improvements	0	2,745	(592)	2,252	64	2,253	(1)	592	
Appleby Magna Caravan site redevelopment	0	39	0	39	0	39	0	0	
Bins and Recycling Containers	194	0	0	194	0	194	0	0	
Commercial Property Works	0	3,499	(3,391)	108	0	108	0	3,391	
CCTV replacement programme	101	44	(50)	95		95	0	50	Moved from development pool to active programme
Public Conveniences	23			23		23	0		New scheme - funded from underspends within the capital programme
Hermitage Access Road	25			25		25	0		New scheme - funded from underspends within the capital programme
Hermitage EcoPark	162			162		162	0		New scheme - funded from external grant income
Development Pool:									
Heritage Assets Work	0	290	(230)	60	1	60	0	230	
Transport Account Vehicles	2,252	3,480	(5,351)	381	35	371	10	5,351	
Hermitage Recreational Ground Building demolition	0	196	(171)	25	1	24	1	146	
Coalville Regeneration	500	345	(720)	25	0	25	0	720	
The Courtyard Roof Repair	200	0	0	200		200	0		
Solar Panels - Leisure Centres	195			195		195	0	0	
UK Shared Prosperity Fund	515	165	(40)	640	0	0	640	0	
Kegworth Public Realm Works	908	0	0	908	0	908	0	0	
Other schemes	0	223	0	223	0	223	0	0	
TOTAL	**6,623**	**13,543**	**(11,654)**	**8,512**	**480**	**7,825**	**687**	**11,679**	

This page is intentionally left blank

Special Expenses 2023/24 Q1 Monitoring & Forecast Outturn Position

COALVILLE SPECIAL EXPENSES	2023/24		
	Budget	Forecast Outturn	Variance
	£	£	£
Parks, Recreation Grounds & Open Spaces	325,520	325,520	0
Broomley's Cemetery & Closed Churchyard	4,860	4,860	0
Coalville in Bloom	0	0	0
Coalville Events	84,440	84,440	0
SPECIAL EXPENSES (NET COST OF SERVICE)	**414,820**	**414,820**	**0**
Service Management recharges/Admin Buildings	99,880	99,880	0
NET COST OF SERVICES AFTER RECHARGES	**514,700**	**514,700**	**0**
Contribution to/(from) Balances/Reserves	(2,402)	(2,402)	0
MET FROM GOVT GRANT & COUNCIL TAX (Budget Requirement)	**512,298**	**512,298**	**0**
FUNDED BY:			
Precept	497,701	497,701	0
Localisation of Council Tax Support Grant	14,597	14,597	0
	512,298	**512,298**	**0**

OTHER SPECIAL EXPENSES	2023/24		
	Budget	Forecast Outturn	Variance
	£	£	£
WHITWICK	13,930	13,930	0
HUGGLESCOTE	18,760	18,760	0
COLEORTON	4,650	4,650	0
RAVENSTONE	480	480	0
MEASHAM	2,550	2,550	0
LOCKINGTON-CUM-HEMINGTON	2,500	2,500	0
OAKTHORPE & DONISTHORPE	4,320	4,320	0
STRETTON	1,440	1,440	0
APPLEBY MAGNA	2,190	2,190	0
OTHER SPECIAL EXPENSES (NET COST OF SERVICE)	**50,820**	**50,820**	**0**
Service Management recharges/Admin Buildings	25,750	25,750	0
NET COST OF SERVICES AFTER RECHARGES	**76,570**	**76,570**	**0**
Contribution to/(from) Balances/Reserves	12,865	12,865	0
MET FROM GOVT GRANT & COUNCIL TAX (Budget Requirement)	**89,435**	**89,435**	**0**
FUNDED BY:			
Precept	88,161	88,161	0
Localisation of Council Tax Support Grant	1,274	1,274	0
	89,435	**89,435**	**0**

This page is intentionally left blank

Appendix 7

2023/24 Special Expenses Earmarked Reserves

COALVILLE SPECIAL EXPENSE RESERVES	Balances 01.04.23	Spend to date	Forecast Spend	Forecast Balance as at 31.03.24
	£	£	£	£
EARMARKED RESERVES				
Local Authority Parks Improvement Programme	15,714	0	15,714	0
Coalville in Bloom	5,000	3,974	5,000	0
	20,714	3,974	20,714	0
PPM EARMARKED RESERVES				
Claremont Drive Play Area Equipment Replacement	8,520	0	8,520	0
Scotlands Recreation - Repairs to potholes	4,054	0	4,054	0
Broomleys Cemetery - Tree works	4,000	0	4,000	0
Broomleys Cemetery - Path repairs (sealing)	3,000	0	3,000	0
Cropston drive play area - Replacement play equip	33,050	0	33,050	0
Sharpley Avenue play area - Replacement play equip	19,660	0	19,660	0
	72,284	0	72,284	0
TOTAL COALVILLE SPECIAL EXPENSE RESERVES	**92,998**	**3,974**	**92,998**	**0**

OTHER SPECIAL EXPENSE RESERVES	Balances 01.04.23	Spend to date	Forecast Spend	Forecast Balance as at 31.03.24
	£	£	£	£
PPM EARMARKED RESERVES				
Hugglescote Cemetery - remove trees, on going tree works	8,120	0	8,120	0
Hugglescote Cemetery - sealing pathways	15,450	0	15,450	0
Hugglescote Cemetery - new trees, remove stumps	3,090	0	3,090	0
Hugglescote Cemetery - decorate Iron Gate	2,060	0	2,060	0
Whitwick Cemetery - tree works	3,088	0	3,088	0
moss, renew path handrail	6,000	0	6,000	0
TOTAL OTHER SPECIAL EXPENSE RESERVES	**37,808**	**0**	**37,808**	**0**

This page is intentionally left blank

Appendix 8

2023/24 HRA QUARTER 1 FORECAST OUTTURN POSITION

HOUSING REVENUE ACCOUNT SUMMARY	Annual Budget	Forecast Outturn	Forecast Variance
	£'000	£'000	£'000
Expenditure			
Repairs & Maintenance	7,693	8,104	411
Supervision & Management	3,995	4,064	69
Provision for Doubtful Debts	100	100	0
Depreciation	3,466	3,466	0
Capital Financing & Debt Management	1,822	1,822	0
Total Expenditure	**17,077**	**17,556**	**480**
Income			
Rent & Service Charges	(19,792)	(19,717)	75
Non-Dwelling Rents	(41)	(41)	0
Other Income	(20)	(20)	0
Investment Income	(286)	(405)	(119)
Total Income	**(20,139)**	**(20,183)**	**(44)**
Net Operating Expenditure/-Surplus	**(3,062)**	**(2,627)**	**436**
Appropriations			
Transfer to/from reserves	3,726	3,726	0
Revenue Contribution to Capital	3,815	3,815	0
Total Appropriations	**7,541**	**7,541**	**0**
NET (SURPLUS)/DEFICIT	**4,479**	**4,914**	**436**

This page is intentionally left blank

Appendix 9

North West Leicestershire District Council
HRA Capital Programme 2023/24

Scheme	Original Budget	Prior Year C/fwd	In-year Changes	Revised Budget	Expenditure @ P3	2023/24 Forecast Outturn	Variance (Revised budget v Forecast Outturn)	Carry-Forward to Future Years
	£'000	£'000	£'000	£'000	£'000	£'000	£'000	£'000
Development Pool:								
Acquisitions and New Build								
Queensway, Measham (Phase 4)		929	(599)	330	0	330	0	599
Howe Road, Whitwick (Phase 4)		823	(823)	0	0	0	0	823
Woulds Court, Moira (Phase 5)		2,089	(2,019)	70	1	70	0	2,019
Cedar Grove, Moira (Phase 5)	460	323	(668)	115	0	115	0	668
The Oaks	1,064	636	(1,625)	75	0	75	0	1,625
Phase 6 - Western Avenue		4	(4)	0	0	0	0	4
S106 purchase - Osgathorpe	0	540	(540)	0	0	0	0	540
S106 purchase - Ravenstone/The Coppice	0	82	(82)	0	0	0	0	82
Acquisition of affordable homes		722	(718)	4	4	4	0	573
EMH - Standard Hill	924	0		924	0	924	0	0
New Sites - Contingency	500	0	0	500	0	500	0	0
Active Programme:								
Improvements and Modernisation								
Home Improvement Programme								
2019 - 2024 Home Improvement Programme	4,500	5,738	(5,738)	4,500	1,068	4,300	200	5,738
Estate Improvements								
Mobility Scooter stores	0	0	0	0	0	0	0	0
Off Street Parking	1,000	220	0	1,220	0	1,220	0	0
Footpaths and Unadopted Roads	50	100	0	150	0	150	0	0
Garage demolition and replacement	100	99	0	199	0	199	0	0
Place Shaping Pilot	0	250	(250)	0	0	0	0	250
Estate Projects - other	100	236	(55)	281	0	281	0	5
Commercial Boilers	150	0	0	150	0	150	0	0
Stock Condition Survey	450	0	50	500	0	500	0	0
Vehicles	55	0	0	55	0	55	0	0
Compliance								
Passive Fire Safety	1,100	0	0	1,100	83	1,100	0	0
Major Aids and Adaptations	400	0	0	400	116	400	0	0
Zero Carbon Programme	3,139	0	(1,439)	1,700	7	1,700	0	1,439
Supported Housing Improvements								
Speech Module	0	260	(260)	0	0	0	0	260
Sheltered Housing Improvements	100	650	(600)	150	0	100	50	600
Scheme Lighting	200	0	0	200	0	200	0	0
Tunstall System	260	0	50	310	0	310	0	0
Electrical Upgrades	0	200	0	200	0	200	0	0
Energy Performance Certificates	130	0	0	130	0	130	0	0
Large Roof Replacement	300	0	0	300	0	300	0	0
Other Capital Spend								
Capital Works - Voids	0	494	(244)	250	0	250	0	244
Housing Management IT System	192	308	0	500	12	500	0	0
Capital Salaries	0	0	0	0	0	0	0	0
Total	**15,174**	**14,703**	**(15,564)**	**14,313**	**1,291**	**14,063**	**250**	**15,469**

This page is intentionally left blank

Appendix 10

Treasury Management – Borrowing and Investments

Borrowing

Table 1 below shows the breakdown of the types of external borrowing held by the Council:

Table 1 – Borrowing summary

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

Since the beginning of the reporting period the Council has paid £81k in interest on borrowing. The forecasted amount to be spent on interest on loans for the financial year 23/24 in total is £2.2m. The overall interest rate on borrowing is 3.6%. There is no change to this budget and spending is in line with expectations.

During the reporting period the Council has not yet paid back any principle on its loans. It is forecasting to repay £2.7m in PWLB loan principle by the end of the year. £1.2m of this is annuity loans whereby regular payments are made throughout the lifetime of the loan and the other is a maturity loan of £1.5m.

The Council also has a Lender Option Borrower Option (LOBO) loan whereby the lender has the option on call dates throughout the year to offer an alternative interest rate. This offer can be taken up by the Authority or the loan can be repaid when that offer is made. The Council holds £3.5m in LOBO loans. Existing procedures are in place for decisive action to be taken in the case of a 'call' to ensure best value for the Council.

The budget for borrowing principle repayments are in line to be met. The only variation that may occur is if the LOBO is called and repaid. This will cause an increase cost pressure of £3.5m in year.

Investments

The breakdown of external investments held by the Council and movement since 31 March 2023 are shown in Table 2 below:

Table 2 – Investment summary

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

5.0.1 The Authority has budgeted £795k in interest income from investments after deductions in 2023/24. Actual income received by 30 June 2023 was £539k. The Council is now forecasting the risk adjusted interest received by 31 March 2024 to be £1.5m and after deductions income to be £1.2m. It is important to note the difficulty in making accurate interest return forecasts in a volatile economic environment. These forecasts is likely to change again over the coming months as such an 80% risk adjustment is placed on anticipated income to avoid overreliance on interest return on budgets.

NORTH WEST LEICESTERSHIRE DISTRICT COUNCIL

CABINET – TUESDAY, 19 SEPTEMBER 2023

Title of Report	**MINUTES OF THE COALVILLE SPECIAL EXPENSES WORKING PARTY**	
Presented by	Councillor Tony Gillard Business and Regeneration Portfolio Holder PH Briefed [X]	
Background Papers	Agenda Document for Coalville Special Expenses Working Party, 15/08/2023 18:30	**Public Report:** Yes **Key Decision:** Yes
Financial Implications	As set out in the reports to the CSEWP on 15 August 2023.	
	Signed off by the Section 151 Officer: Yes	
Legal Implications	Legal advice was provided during the drafting of all reports to the CSEWP on 15 August 2023.	
	Signed off by the Monitoring Officer: Yes	
Staffing and Corporate Implications	There are no staffing or corporate implications arising from the report.	
	Signed off by the Head of Paid Service: Yes	
Purpose of Report	To share the minutes of the Coalville Special Expenses Working Party from 15 August 2023.	
Reason for Decision	So that the decisions of the Coalville Special Expenses Working Party can be considered.	
Recommendations	**THAT CABINET:** **1. NOTES THE MINUTES OF THE COALVILLE SPECIAL EXPENSES WORKING PARTY AT APPENDIX 1.** **2. CONSIDERS ANY RECOMMENDATIONS MADE BY THE WORKING PARTY AT ITS MEETING ON 15 AUGUST 2023.**	

1.0 BACKGROUND

1.1 The Coalville Special Expenses Working Party consists of all ward members from the Coalville Special Expenses Area and meets as often as is required to meet business demands, which is usually quarterly.

1.2 As the Working Party reports directly to Cabinet, all recommendations made are to be sent to the first available Cabinet meeting for final approval.

2.0 TERMS OF REFERENCE

2.1 To consider budget and financial issues which either solely or predominantly affect the Coalville Special Expenses Area and to make recommendations to Cabinet.

2.2 To receive reports and examine possible project options on which recommendations will be made to Cabinet.

3.0 RECOMMENDATIONS TO CABINET FROM THE MEETING ON 15 AUGUST 2023

3.1 Finance Update

3.1.1 No recommendations were made.

3.2 Events Update

3.2.2 No recommendations were made.

Policies and other considerations, as appropriate	
Council Priorities:	Insert relevant 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:	Taken into consideration in drafting of reports to CSEWP.
Safeguarding:	Taken into consideration in drafting of reports to CSEWP.
Equalities/Diversity:	Taken into consideration in drafting of reports to CSEWP.
Customer Impact:	Taken into consideration in drafting of reports to CSEWP.
Economic and Social Impact:	The reports and proposals presented to CSEWP will have positive economic and social impacts.
Environment, Climate Change and Zero Carbon:	Taken into consideration in drafting of reports to CSEWP.

Consultation/Community/Tenant Engagement:	Taken into consideration in drafting of reports to CSEWP.
Risks:	None identified.
Officer Contact	Paul Wheatley Head of Business and Regeneration Paul.Wheatley@nwleicestershire.gov.uk

This page is intentionally left blank

MINUTES of a meeting of the COALVILLE SPECIAL EXPENSES WORKING PARTY held in the Abbey Room, Stenson House, London Road, Coalville, LE67 3FN on TUESDAY, 15 AUGUST 2023

Present: Councillor M B Wyatt (Chair)

Councillors D Everitt, M French, J Geary, J Legrys, J Windram and L Windram

Officers: Mrs A Crouch, Mrs C Hammond, Mr P Wheatley, Mr T Devonshire and Ms S Thirkettle

9. APOLOGIES FOR ABSENCE

Apologies were received from Councillor M Burke and J Page.

10. DECLARATIONS OF INTEREST

Councillor J Legrys declared a registerable interest in all items as a volunteer at Hermitage FM.

Councillor J Geary declared a registerable interest in all items as Director of the

Springboard Centre and as the Council's representative for Coalville Town Football Club. Councillor M Wyatt declared a registerable interest in all items as the owner of two businesses in Coalville.

11. MINUTES OF THE PREVIOUS MEETING

It was moved by Councillor J Geary, seconded by Councillor M Wyatt and

RESOLVED THAT:

The minutes of the meeting held on 13 June 2023 be confirmed as an accurate record of proceedings.

12. COALVILLE SPECIAL EXPENSES FINANCE UPDATE

The Finance Team Manager presented the report.

In response to a question about the nature of the briefing set out in the report at 3.7, the Head of Finance confirmed that the briefing session would inform members on the current position and aid the Working Party in setting the budget for next year. It would also, she added, be aimed at clarifying any questions newly elected members of the Working Party may have.

The Head of Property and Regeneration added that information would be provided ahead of the briefing about the implications for the Working Party's budget, with regards to maintaining land at the junction of Broomleys Road.

In response to a question about what appendix A represented, the Head of Finance advised that this was for the previous financial year, and represented significantly less coming from the reserves than originally envisaged, although anything at all coming from the reserves was undesirable. This year the position was even healthier than that, she added, and it was envisaged that a much smaller figure would be needed from the reserves. The Finance Team would also work to improve this further.

It was moved by Councillor J Legrys, seconded by Councillor J Geary and

RESOLVED THAT:

1. The 2022/23 provisional outturn figures and Coalville Special Expense balances as at 31 March 2023 be noted.

2. The 2023/2024 Quarter 1 budget monitoring figures and forecasted outturn as at Quarter 1 for 2023/2024 be noted.

3. That a briefing take place with members of the Working Party during September to provide further details on the information contained within the report.

13. 2023/24 EVENTS UPDATE

The Head of Property and Regeneration presented the report.

In response to a question about how the £20,000 cost for Picnic in The Park was calculated, the Head of Finance advised that it was the net figure, and consequently included all income received for the event.

The Chair requested that next year the incoming money for the event was explicitly noted – the Head of Finance was happy for to proceed with this suggestion going forwards.

Following on from this a member requested going forwards a balance sheet be produced for each future event for the Working Party to examine – the Chair concurred, and Officers were happy to proceed with this suggestion going forwards.

In response to a question about the time span for when the light columns would fail, the Head of Property and Regeneration advised that this year they would be fine, next year they would stress test again, and if failures continued at the current rate the light columns could well prove to be unviable.

In response to a question about Marlborough Square and the November deadline, the Head of Property and Regeneration advised that the contractor would suspend work a week before the Christmas celebrations, in a manner most conducive to public safety and leisure. He added that he was awaiting further clarification on certain matters from the contractors. It was unlikely that there would be a Christmas tree or lights in Marlborough Square this Christmas.

In response to a question about Christmas activities at Newmarket and how these would be impacted by the work on Marlborough Square, the Head of Property and Regeneration advised that they would have to assess this nearer to the time, with an emphasis when making that decision on public safety.

In response to a question about Needhams Walk car park and whether permission had been attained to close it, the Head of Property and Regeneration advised that they were working with the organisation who owns the car park.

In response to a question about contingencies should the Christmas event at Needhams Walk be cancelled, the Head of Property and Regeneration accepted the concerns, but advised that the Council was dependent on relations with third parties, which were subject to fluctuations over time. There could therefore be no guarantees, but contingency plans would be put in place. On a longer term basis, the Marlborough Square project would provide the organisation with a pedestrianised public space. He then illuminated the considerations behind event planning in the town when the available space was considered.

In response to a question about stress testing the light columns, the Head of Property and Regeneration set out how it worked and invited members to join him if they wanted to see this in greater detail.

Several Members commended Officers for the Coronation event and Picnic in the Park.

A couple of Members wondered about the feasibility of bussing the public into the town for celebrations. The Head of Property and Regeneration advised that Officers had been looking at using County Council car parks and would approach them about other car parks Members had suggested.

Following a discussion amongst members, Officers clarified that the recommendations of the report the Working Party were voting on superseded the discussions of the Events Working Group. Therefore, after all Members affirmed that they did want the fun fair to go ahead, it was accepted that there was no need to amend the recommendations as this was already reflected within the report.

Several Members expressed their regrets at the damage done recently to Coalville Park and praised the work of the Parks Team in dealing with the matter.

It was moved by Councillor M Wyatt, seconded by Councillor J Geary and

RESOLVED THAT:

That progress made against the 2023/24 Events and Christmas Lights Programme be noted.

The meeting commenced at 6.30 pm

The Chairman closed the meeting at 7.22 pm

Chairman's initials

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank