Appendix 2

Information Security Policy

Item	Details
Reference:	Information Governance-1-ISP
Status:	Final
Originator:	Head of Legal and Support Services
Owner:	ICT Manager
Version No:	1:1
Date:	5 January 2026

Key policy details

Approvals

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

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

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

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

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

Policy Location

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

Equality Impact Assessment (EIA)

Completed by	Completion date
Fay Ford	August 2024

Revision History

Version Control	Revision Date	Summary of Changes
1:1	24 September 2024	Creation of Document
1.2	5 January 2026	Revised

Policy Review Plans

This policy is subject to a scheduled review once every year or earlier if there is a change in legislation or local policy that requires it.
This policy will be reviewed annually, or sooner should significant events or developments necessitate an update.

Distribution

Title	Date of Issue	Version No.
Distributed to Cabinet	24 September 2024	1:1
Published on NWLDC Website	27 September 2024	1:1

Information Security Policy

1. Introduction

This Information Security Policy outlines the Council's commitment to protect North West Leicestershire District Council's ("The Council") information assets against all internal, external, accidental or deliberate threats and minimise risks related to information security. Information is a critical asset for the Council. The security of information assets, as well as the supporting processes, systems and networks, is essential to maintaining operational effectiveness, reputation, financial accuracy and legal compliance.

The Council is subject to a wide variety of sophisticated security threats, including malware, hackers and computer-assisted fraud. The dependence on data, information systems and services means that the Council is vulnerable to these threats.

The requirement to interconnect the Council's network with suppliers and partners, alongside the growing use of Cloud services, makes security increasingly complex.

Information security is characterised as the preservation of:

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

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

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

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

This document should be read in conjunction with the Council's ICT and Security Procedure.

2. Scope

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

Application of this policy applies throughout the information lifecycle from acquisition/creation, through to utilisation storage and disposal. It should be read in conjunction with the Council's internal procedures, including the ICT Cyber and Security Procedure.

3. Responsibilities

The Senior Information Risk Owner (SIRO)

- is responsible for managing Information Security within the authority.

The IT Manager

- is responsible for the implementation of this policy.

All employees

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

4. Authorised Use

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

5. Acceptable use

All users of ICT systems and information for which the Council is responsible must agree to, and abide by, the terms of the Council's Internet and Email Access – Conditions of Use policy document.

6. Information Classification

All information must be handled in a way appropriate to its sensitivity, in accordance with the Information Classification Procedure.

7. Access Control

The Council will ensure that:

- Users are only granted access to the IT systems and data necessary to fulfil their role;
- Remote access services are configured to minimise opportunities for unauthorised access or denial of service;
- All IT equipment is adequately secured to prevent theft and critical IT infrastructure is physically secured to prevent unauthorised access;
- All IT systems are designed, configured and managed to minimise opportunities for unauthorised access or denial of service;
- The use of passwords is managed to minimise the risk of unauthorised

access to IT systems or data;
- Controls are applied to prevent unauthorised access to information stored on removeable media; and
- Third party access to Council systems is authorised and controlled and third parties with such access must adhere to the Information Governance Framework, including other information governance policies.

8. IT Software and Equipment

The Council will ensure that:

- All hardware and software is kept up to date to minimise the likelihood of security vulnerabilities being exploited;
- IT equipment is properly configured and managed to reduce the risk of malware and other security threats;
- Resources are hosted in cloud computing environments that are maintained to an acceptable level of security as deemed by the ICT Team Manager;
- All software is licences and only installed by IT staff;
- Controls are implemented to reduce the risk to the confidentiality, integrity and availability of IT systems and data caused by malicious software (malware);
- Systems are monitored to ensure malicious activity is detected; and
- Controls are implemented to minimise the impact of any system unavailability;
- Procedures are implemented to minimise the Council's exposure to fraud, theft or disruption of its systems such as segregation of duties, dual control, peer review or staff rotation in critical susceptible areas; and
- Data protection is integrated into the Council's processing activities and business practices from the design stage right through the lifecycle (data protection by design and by default); and
- Data is held on a network directory where possible and that routine backup processes capture the data.

9. Incident Response

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to Council assets, or an event which is in breach of the Council's security procedures and policies. All Council employees, councillors, agency staff, contractors, volunteers or any other persons who have access to, or use the Council's information systems and data have a responsibility to report security incidents and breaches of this policy as quickly as possible through the Council's Data Breach and Information Security Incident Procedure. The Council will take appropriate measures to remedy any breach of the policy and its associated procedures and guidelines through the relevant frameworks in place. In the case of an individual then the matter may be dealt with under the disciplinary process and advice will be sought from the Council's Human Resources team.

10. Security Training and Awareness

The Council is committed to promoting safe working practices. All employees will receive security awareness training commensurate with the classification of information and systems to which they have access. Staff working in specialised roles will receive

appropriate training relevant to their role. Relevant information security policies, procedures and guidelines will be accessible and disseminated to all users. It remains the employees' responsibility to ensure they are adequately informed of information security policies and procedures.

11. Compliance with Legal and Contractual Obligations

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

- Data Protection Act 2018
- UK General Data Protection Regulation 2018
- The Freedom of Information Act 2000
- The Environmental Information Regulations 2004
- The Computer Misuse Act 1990
- The Human Rights Act 1998
- The Copyright Designs and Patents Act 1988