Appendix 9

Information Security Policy

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

Key policy details

Approvals

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

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

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

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

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

Policy Location

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

Revision History

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

Policy Review Plans

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

Distribution

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

Information Security Policy

1. Introduction

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

Information security is characterised as the preservation of:

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

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

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

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

2. Purpose

The purpose of this policy is to:

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

3. Scope

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

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

4. Responsibilities

The Senior Information Risk Owner (SIRO)

- is responsible for managing Information Security within the authority.

The IT Manager

- is responsible for the implementation of this policy.

All employees

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

5. Authorised Use

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

6. Information Classification

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

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

7. Data Retention

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

8. Access Control

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

longer necessary.

9. Password Management

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

10. Data Encryption

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

11. Incident Response

- All security incidents shall be reported immediately to the ICT Service Desk who will pass the calls to the ICT Security Officer or ICT Manager who will instigate an investigation and report any incidents that cause serious loss or damage to the Head of Customer services and the Data protection officer.
- The personal data breach process and reporting requirements still apply to security incidents that amount to or include personal data breaches. Any Security incident that may have potential to lead to disciplinary action will involve the appropriate involvement and consultation with head of Human Resources and Organisation Development and or (depending on the nature of the incident) the Audit services manager.

12. Physical Security

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

13. Training and Awareness

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

14. Third-Party Vendors

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

15. Compliance with Legal and Contractual Obligations

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

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

- The Copyright Designs and Patents Act 1988

Compliance

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

Regular audits will assess adherence to this policy.

Equality Analysis

Completion of Equality Impact Assessment (EIA) Form

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