Information Governance Framework

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

Key policy details

Approvals

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

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

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

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

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

Policy Location

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

Equality Impact Assessment (EIA)

Completed by	Completion date
Fay Ford	1 June 2024

Revision History

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

Policy Review Plans

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

Distribution

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

Information Governance Framework

1. Introduction

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

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

2. Scope

This Information Governance Framework and the documents within it apply to all staff including employees, councillors, agency staff, contractors, volunteers or any other persons who have access to, or use the Council's information. It applies to all types of information and data, both electronic and manual, which is held, processed or transmitted by the Council.
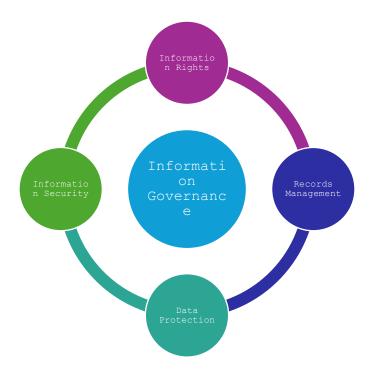
Information includes all paper and electronic records, whether that be raw or analysed data, informal or formal documents, customer or other records and any other type of content.

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

3. Principles

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

1. Information Rights - we have legal obligations to provide information when requested.

2. Records Management - we must retain information for an appropriate period of time and manage records effectively.

3. Data Protection - we are required to have appropriate safeguards in place to protect our information, especially personal data.

4. Information Security - we must ensure that we have technical measures in place to ensure that the handling of our information is secure.

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

4. Policies and Procedures

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

1. Information Rights Policy

2. Records Management Policy

3. Data Protection Policy

4. Information Security Policy

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

Information Governance Framework

Policies

These set out why requirements are in place

Our key policies are:

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

Standards

These set out what the requirements are

These include:

Retention Schedule
Information Asset Register
Data Sharing Register
Acceptable Use

Procedures and Guidance

These set out how requirements are met

These include:

Date Breach and Information Security Incident Procedure

Information Requests Guidance

Procedure for Infomation Sharing

Subject Access Requests Guidance

CCTV and Surveillance Camera Technologies Procedure

Employee Monitoring Procedure

5. Roles and Responsibilities

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

The SIRO has the following responsibilities:

- To be accountable for risk management in relation to information governance at the Council;

- To take overall ownership of the organisation's information risk approach, including the information governance framework; and

- To oversee the Data Breach and Information Security Incident Procedure and the Council's compliance in relation to dealing with information security incidents (data breaches).

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

- To monitor compliance across the organisation to ensure that the Council meets its obligations under data protection legislation and applicable guidance;

- To ensure that the Council develops, implements, reviews and updates measures to comply with data protection legislation;

- To ensure that the Council has an appropriate training programme to make members of staff aware of their responsibilities in relation to information governance and data protection;

- To deal with any complaints in relation to the processing of personal data;

- To be responsible for the Council's approach to dealing with information security incidents and ensure that any personal data breaches are fully investigated and reported through the appropriate channels if appropriate; and

- To act as the contact point for the ICO on issues relating to the processing of personal data and to co-operate with the ICO in relation to any enquires and/or investigations.

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

Information Asset Owners

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

Surveillance Camera System Senior Responsible Officer

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

IT Security

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

6. **Training and Guidance**

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

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

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

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

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

7. **Monitoring and Review**

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

8. **Relevant Legislation**

The following legislation is relevant to this Information Governance Framework:

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