



# Records Management Policy

Item	Details
Reference:	Information Governance -1-RMP
Status:	Final
Originator:	Head of Legal & Support Services
Owner:	Data Protection Officer
Version No:	1:2
Date:	24 September 2024

## 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
Consulted with Internal Audit	October 2025	1:2

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.
- **Legislation and 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 NWLDC’s website and on the Sharepoint page under current policies tab.

### Equality Impact Assessment (EIA)

Completed by	Completion date
Fay Ford	August 2024
Laurent Flinders	October 2025

### Revision History

Version Control	Revision Date	Summary of Changes
1:1	July 2024	Creation of Document
1:2	October 2025	Updated Legislation Data (Use and Access) Act 2025 Amendment made to the Information Asset Owners (IAO) roles and responsibilities.

### 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	27 September 2024	1:1

## Records Management Policy

### 1. Introduction

North West Leicestershire District Council's ("The Council") records support effective service delivery, provide evidence of its activities and decisions, helps the Council to make informed decisions, comply with relevant legislation, meet business and regulatory requirements and maintain the corporate memory. It is important that the Council manages its records appropriately to ensure that it complies with data protection legislation and is able to locate information when required. Systematic management of records protects the Council's most important information and improves business resilience and efficiency.

This policy establishes guidelines for the management, retention and disposal of data records within the Council. It sets out the Council's lifecycle approach to records management and the expectations for all employees in managing information effectively.

### 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.

This policy applies to all records that the Council holds, including the following:

- Documents (including hand-written, typed, and annotated copies).
- Paper based files.
- Computer files (including word processed documents, databases, spreadsheets and presentations).
- Maps and plans.
- Electronic mail messages (email).
- Web pages (on either the intranet and internet).
- Faxes.
- Brochures and reports.
- Forms.
- Audio and video tapes including CCTV and voicemail / voice recording systems.

### 3. Use

All information must be used consistently, only for the intentions for which it was intended and never for an individual employee's personal gain or purpose. If in doubt employees should seek guidance from the Data Protection Officer.

**Disclosure** - only specific information required should be disclosed to authorised parties and always in accordance and with strict adherence to the Data Protection Act. There are a range of statutory provisions that limit, prohibit or set conditions in respect of the disclosure of records to third parties and similarly arrange of provisions that require or permit disclosure.

### 3.1 Storage of Records

There is an Information Asset Register/ Record of Processing Activities.

The Council has an Information Asset Register/ Record of Processing Activities that identifies the assets owned by the Council and location of the same. It is subject to annual review and any risk found will be reported to the Senior Information Risk Owner (SIRO).

### 3.2 Retention

The retention period varies dependant on the type of information being stored. All NWLDC Records retention periods should be detailed in the Information Asset Register and can be checked in the Corporate Retention Schedule available as part of the Council's Information Governance Framework.

The information must be relevant, fit for purpose it was intended and only retained for as long as it is genuinely required.

**3.3 Disposal** - It is particularly important under Data Protection legislation that the disposal of records, which is defined as the point in their lifecycle when they are either transferred to an archive or destroyed, is undertaken in accordance with clearly established policies which have been formally adopted by the Council.

**3.4 Transfer** - The mechanisms for transferring information from one organisation to another should be tailored to the sensitivity of the material contained within the records and the media on which they are held. The DPO can advise on appropriate safeguards.

## 4. Relevant Legislation

The Council is committed to continuously improving the way it responds to information requests that fall under specific statutory regimes.

The UK General Data Protection Regulation  
The Data Protection Act 2018  
The Freedom of Information Act 2000  
The Environmental Information Regulations 2004  
The Data (Use and Access) Act 2025

The following legislation is also relevant to this policy:

- Human Rights Act 1998
- The Local Government (Records) Act 1962 - this gave Local Authorities limited discretionary power to hold their records in local archives
- The Local Government Act 1972 - sets out the basic requirement for local authorities to 'make proper arrangements' to keep good records

## 5. Information Management Framework

The Council has implemented a framework of processes, procedures, standards and training materials together with defined roles and responsibilities that has been established, in order to support compliance with this policy so that:

- i) Appropriate information and documents are captured as records;
- ii) Records can be easily accessed by those who need them;
- iii) Records are available for as long as they are required in accordance with legislation and listed;
- iv) Records are disposed of appropriately when no longer required in line with legal and regulatory obligations;
- v) Records will be appropriately marked and kept securely and protected from accidental loss or destruction.

## **6. Roles And Responsibilities**

### **The Senior Information Risk Owner (SIRO)**

The Council has appointed the Monitoring Officer as the SIRO. The SIRO has responsibility for ensuring that effective systems and processes are in place to address the Information Governance agenda.

The SIRO is the overall owner of the information risk within the Council and acts as the focal point for information risk management within the Council including resolution of any risk issues raised by IAO. The SIRO will report annually to the Audit and Governance Committee on the content of the SIRO Report regarding information risks.

### **Information Asset Owners (IAO)**

Each Information Asset will have a relevant team manager as an Information Asset Owner.

The information asset includes records associated with the operation of the directorate function. Key decisions about the management of information will be made by the IAO.

### **Data Protection Officer (DPO)**

The DPO appointed under statutory General Data Protection Regulation (GDPR) obligations, is responsible for monitoring the Council's compliance with data protection legislation and its compliance with its own policies in relation to the protection of personal data. Monitoring of this policy will be overseen by the DPO. In the event of identification of high risks, the DPO will escalate to the appropriate level of management.

### **All Staff**

All Council employees are responsible for any records that they create or use in the course of their duties. It is the responsibility of all employees to adhere to this policy when handling all types of Council information.

Official

This document is official, handle appropriately