LANCASTER CITY COUNCIL

Promoting City, Coast & Countryside

RECORDS MANAGEMENT POLICY AND RETENTION SCHEDULES

Document Control

Approved by:	Senior Leadership Team	**Date:**	07.02.2023
Document location:	[redacted]		
Document owner:	Information Governance Manager		
Review period:	2 years		
Next review date:	August 2024		

Revision History

Version	Date	Reviewed By	Amendment Details
V4.01	24/08/2022	[redacted]	Overhaul of policy, procedure, legislation and Retention Schedules

CONTENTS

1 Introduction

The Council creates, uses, and receives records which are a valuable resource and an important asset, supporting its legal, financial, business and administrative requirements.

The systematic management of the Council's records, from creation to disposal, is essential to protect and preserve them as evidence of actions, to support present and future activities and business decisions, and to ensure accountability to present and future stakeholders. Furthermore, effective records management is central to upholding the Council's obligations under information legislation.

The Records Management Policy sets out the Council's commitment to consistently and securely create, keep, and dispose of high-quality records documenting its business and activities.

It sets out the principles of good records management which shape the development of operational procedures. The policy also defines the characteristics of high-quality records, and describes the mechanisms of planning, governance and training which support compliance with the policy.

2 Purpose

The purpose of the records management function is to:

- Create and capture authentic and reliable records which provide evidence of the Council's activities and decisions and which demonstrate its accountability
- Secure, maintain and preserve those records for as long as they are required and to provide access to them as necessary to support the Council's operations and fulfil its statutory obligations
- Identify those records which will form a significant part of the historical record of the Council's activities and make provision for their permanent or long- term preservation
- Identify those records that are vital to the continuance of Council's business and protect them against disaster
- Destroy records that are no longer required, having regard to statutory recordkeeping requirements, thus promoting the efficient use of physical and electronic storage space, and negating malicious or accidental data loss
- Respond to ad-hoc "legal hold" requests that may override default retention periods for particular records

3 Legislative Framework

The Records Management Policy has been created with reference to the following legislation and standards:

3.1 Legislation

- Data Protection Act 2018 (DPA)
- Electoral Registration and Administration Act 2013
- Environmental Information Regulations 2004 (EIR)
- Finance Act 2020
- Freedom of Information Act 2000 (FOIA)
- General Data Protection Regulations 2016 (GDPR)
- Human Rights Act 1998
- Limitation Act 1980
- Local Government (Access to Information) Act 1985
- Local Government Act 1972
- Prevention of Social Housing Fraud Act 2013
- Public Records Act 1958 and 1967

- Public Service Pensions Act 2013
- Regulation of Investigatory Powers Act 2000
- Telecommunications (lawful business practices) and (interception of communications) Regulations 2000

3.2 Standards

- ISO 15489 Information and Documentation – Records Management
- ISO 27001:2013 Standard for Information Security Management
- Section 61 Code of Practice on Records Management

These lists are not exhaustive and in addition managers need to identify and comply with legal obligations and professional standards pertinent to their business area and the information they capture, store, and use.

4 Intended Audience

All members of staff are responsible for ensuring that records in their care are properly managed.

5 Scope

In records management it is important to be clear about the difference between a document and a record.

A document is any piece of written information in any form, produced or received by an organisation or person. It can include databases, website, email messages, word and excel files, letters, and memos. Some of these documents are ephemeral or of very short-term value.

Some documents will need to be kept as evidence of business transactions, routine activities or as a result of legal obligations, such as policy documents. These are official records.

In other words, all records start off as documents, but not all documents will ultimately become records.

For the purposes of this policy, a record is defined as:

- Recorded information, regardless of media or format, created or received in the course of individual or organisational activity, which provides reliable evidence of policy, actions or decisions (National Archives)

The Records Management Policy applies to:

- records created and received by all departments and/or services, in all formats, both paper and electronic
- records stored in any electronic or physical repository

The Records Management Policy applies only to records, not to documents.

6 Policy Statement

Effective management of current and historic records supports the business of the Council. In practice this means that:

- Accurate and robust record-keeping allows the Council reliably to identify people in need and provide them with the services they require quickly and efficiently, ensuring resources are directed where they are needed most

- Good records management supports cost-effective and efficient business operations, freeing up valuable staff time to focus on the best possible frontline service delivery
- By keeping records accurate and up to date, we ensure that reports on outcome indicators draw on authoritative information, thus supporting the Council to successfully achieve their targets
- Sound recordkeeping practice supports partnership working with both service users and other public service providers, enabling productive working relationships while still protecting the Council against risks of information loss and/or unauthorised access to Council's information
- Identification of business-critical records and effective disaster management and preparedness regarding records and information are essential to ensuring the long-term sustainability of Council business

The Council accepts the following core principles as essential to maintaining effective records management across the organisation. These principles apply to the management of all records, whether paper or electronic:

- Records management is recognised as a core corporate function
- Records management policies and procedures are applied consistently across the Council
- Records management is included in a governance framework with clearly defined roles and lines of responsibility
- Records are mapped to business functions and activities
- Records are created according to agreed forms and structures
- Records are created with associated metadata, which is persistently linked and managed
- Records are kept in systems that enable them to be stored, retrieved, used, and shared as necessary
- Sufficient planning and resources are devoted to preserving records and making them accessible over time, particularly in the case of business-critical records
- Records are maintained in a safe and secure environment, where access to them is controlled
- Records are retained only for as long as they are required, and the Council can explain why records are no longer held
- Record-keeping practice complies with legal and regulatory requirements, applicable standards and organisational policies, and compliance is regularly monitored and assessed
- Proper arrangements are made for the long-term preservation of and access to materials of historic significance

Records contain evidence of the Council's business transactions and/or information relating to those transactions. Records can also contain information the Council requires as part of its legal obligations. It does not matter what format the record is in; a record can be an email, a file, a database, or any other format. What matters is the information the record holds.

In order to support business effectively, it is important to keep high quality records. To be considered 'good', a record should have the following characteristics:

- Authenticity: the record is what it claims to be and has not been tampered with. It can be relied on as evidence, for example in court
- Reliability: the contents of the record can be trusted as a full and accurate representation of the Council's transactions and activities
- Integrity: the record is protected against unauthorised alteration. Any authorised changes are clearly indicated and traceable
- Useable: the record can be located, retrieved, presented and interpreted. Links between related records should be clear. It should be easy to determine what activity or department created the record

7 Ownership

All records created and received by the Council, and its external service providers where they are processing information on the Council's behalf, who create, receive and use records, are the property of the Council, and must not be used for any activity or purpose other than official Council business.

8 Positions responsible for compliance

All staff who create, receive or use records will have some responsibility for their management. Specific responsibilities are outlined below:

- **Information Governance, Cyber Security and ICT User Group (IGCSICTG)**

The Information Governance, Cyber Security and ICT Group (IGCSICTG) is made up of senior Information Governance and IT leads and nominated officers from each Council Service and has responsibility for the Information Governance, Cyber Security and ICT arrangements across the Council. The IGCSICTG's role is to drive forward delivery of the Information Governance Improvement Programme which forms the basis of the Information Governance Framework. The IGCSICTG also has oversight of compliance issues reported to it via the ICT and IG Manager's Group.

Each Service's nominated Officer is responsible for disseminating information, instructions and guidance to their Service on behalf of the IGCSICTG and escalating any areas of concern to them.

- **Information Governance Manager**

In the context of this policy, the Information Governance Manager is responsible for:

- Ensuring that the management of the Council's records complies with legal and professional obligations
- Managing records in designated corporate records management systems
- Advising Council officers on records management
- Implementing the Records Management policy
- Maintaining the Corporate Retention Schedule

- **Data Protection Officer**

The Data Protection Officer (DPO) is responsible for advising, monitoring and reporting the Council's compliance with the General Data Protection Regulations (GDPR) and any relevant UK legislation (eg Data Protection Act). Formal duties are defined by GDPR and include raising awareness of data protection requirements, leading information audits, advising on and reviewing data protection impacts and information sharing and investigating data breaches and incidents.

The DPO is also the first point of contact for the Information Commissioner's Office and for individuals whose data is processed by the Council.

- **Information Asset Owners**

Information Assets are identified and recorded on the Information Asset Registers. Information Asset Owners are nominated for all of the Council's Information. They are responsible for ensuring that: their systems are documented and managed appropriately to guard against operational failures; security requirements are included in any changes to their system; only appropriate staff have access to their system and there are documented contingency plans for their system; any network links are protected appropriately and systems are protected against viruses; and system users are aware of their responsibilities for security and their system is monitored and audited to check for

security breaches. They are also responsible for ensuring the publication of data relating to their asset (including on the Council's website) is accurate and up to date.

- **Service Heads**

All Service Heads and Team Leaders will be responsible for ensuring:

  - the records management policy is implemented and complied with in the department or service under their control
  - staff receive training, development and support in records management matters
  - all records within the department have an identified owner, responsible for their management whilst in use
  - adherence to proper procedures to ensure that no unauthorised destruction of records occurs, particularly any wilful destruction of records pertinent to a request made under the Freedom of Information Act, Environmental Information Regulations or the Data Protection (Subject Access Request) legislation
  - a satisfactory audit trail exists for records destroyed according to the retention and disposal schedules
  - records of long- term importance are offered to the Local History/Archives Service for permanent storage
  - business recovery plans are in place to allow continuity of service in event of a disaster

- **Individual officers**

All records created by officers during the course of their work are the property of the Council. Individual officers are responsible for:

  - Adhering to corporate and any directorate records management policies
  - Filing records according to a file structure appropriate to their subject and format to enable ready retrieval when required
  - Ensuring that all records, regardless of format, are stored safely in suitable conditions
  - Ensuring that records are retained in accordance with the retention schedules and disposed of according to corporate and directorate policies when their retention period has expired

Non-compliance could result in the Council being put at risk of legal challenge, service users being put at risk, colleagues being inconvenienced with their time wasted and Council resources being wasted.

Actions or neglect leading to a breach of this policy by an employee could result in disciplinary action

9 Retention Schedule

The Council's Retention Schedule has been created to support the Council to meet their statutory obligations to ensure that information is retained for the correct period and then disposed of appropriately. A copy of the Retention Schedule can be found at **Appendix 1**.

It is unlawful to retain personal information for longer than necessary. If any delay is anticipated, then this should be raised with the Data Protection Officer with a timescale for when the information will be disposed of.

The Retention Schedule sets out how long information should be kept before it is disposed of or, where it is deemed to be of permanent historical value, transferred to the Local History/Archives.

Staff should seek guidance from line managers in departments, or the Data Protection Officer, if they feel that any changes/ modifications/ additions to the schedule are required.

The Retention Schedule applies to any format which Records, or Information may come in, digital or physical. Information that has reached the end of its retention period should be disposed of securely without delay.

Documents are not covered by the Retention Schedule. They need to be destroyed as soon as they become obsolete. In broad terms, documents are of a routine or trivial nature; have little administrative value, and only needed for a limited period. Documents include, but are not limited to:

- copies of records used for reference purposes only
- rough drafts of committee reports not circulated to other staff and of which a final draft has been produced and captured as a record. NB: Versions of drafts which contain significant changes to the context must be captured as records
- E-mails giving minor instructions of a routine nature that are used to further some activity
- working papers, background notes and reference materials used to prepare or complete other documents

Any records destruction must be documented, either automatically by an audit trail, or manually by completing a Destruction Log, a template Destruction Log can be found at **Appendix 2.**

It is essential to take into consideration the format and the sensitivity of the information when deciding on the appropriate disposal method. When information is disposed of without an automated audit trail a Destruction Log shall be completed, retained by the service and forwarded annually to the Information Governance Manager so that sufficient descriptive details can be retained to enable accurate reporting on the information that has been destroyed.

Information may sometimes be kept in error because of technical problems, human error or by deliberate act. Information kept in error must always be reported, on discovery, to the Information Asset Owner to allow them, in collaboration with the Data Protection Officer, to decide what action needs to be taken.

Wrongful disposal may occur because of technical problems, human error or by deliberate act. Wrongful disposal of information must always be reported, on discovery, to the information owner to allow them to identify any gaps in their information sets and to allow them, in collaboration with the Data Protection Officer, to take the decision as to what action needs to be taken and whether the Data Breach procedure needs to be instigated.

All staff, partners and contractors will adhere to the Council's Information Security Policies and, in relation to partners and contractors, any contractual or Data Sharing Agreement requirements, when disposing of or transferring information in any format including hardcopy, electronic and information contained on mobile storage devices.

The Council's Retention Schedule indicates the sort of records that should be offered to the Local History/Archives Service. Where such a record is in electronic format, consideration should be given to the potential longevity of that format.

9.1 Suspending the disposal of records

If an officer feels there is a reason to suspend the disposal of a record, they should call and speak to the Information Governance Team for advice before making a decision – there may be a valid reason for this record to be kept longer than originally anticipated but advice should always be sought.

10 Training and Awareness

As all Council employees are involved in creating, maintaining, and using records it is vital that they all understand their records management responsibilities as set out in this policy. Managers must

ensure that all their staff are aware of their obligations regarding Data Protection, Freedom of Information, and Records Management. Training on Information Governance and Security is mandatory for all staff and is required to be refreshed every 2 years.

11 Policy Review

This policy will be updated every 2 years or as necessary to reflect best practice and to ensure compliance with any changes or amendments to relevant legislation.

Appendix 1: Retention Schedule (example)

[Service Area]

Retention schedule reviewed and agreed by:

Name	Signed	Position	Date

Record Type – Description and examples	Storage media	Retention Period	Reasoning
Example			
Plans and testing Decision Making Logs Emergency Plans General Incident Logs	Electronic	Revise annually, anonymise previous versions after 3 years if archiving	Best practice
Financial Accounting Preparation of Annual Report and Accounts Expenditure and receipts and revenue	Electronic	Current Financial year + 6 years Current Financial year + 4 years	Limitation Act 1980

Appendix 2: Template Destruction Log

Records Destruction/Deletion Form - Service Name [*DRAFT* *SAMPLE*]

New Destruction/Deletion Event (Date/Year)

Ref/Code	General Description of Records	Covering Dates/Closure Period	Hard Copy (paper) records included (Y/N)?	Digital Records* included (Y/N)?	Comments (if any)*	Actioned by	Date Actioned
COL1.29	Annual Leave forms	2000-2014	Y	N	Forms held in paper copy only	JMC	01.02.202
					Quantity of hard copy records destroyed (bags, boxes):	**2 Bags**	

Appendix 3: Records Management Lifecycle