



CITY OF
Lincoln
COUNCIL

Records Management Policy



CITY OF
Lincoln
COUNCIL

Document Control

Organisation	City of Lincoln Council
Title	Information Sharing Policy
Author – name and title	Becky Scott, Legal & Democratic Services Manager
Owner – name and title	Becky Scott, Legal & Democratic Services Manager
Date	July 2018
Approvals	July 2018 - Executive
Filename	Records Management Policy
Version	V.1.1
Protective Marking	Not Protectively Marked
Next Review Date	July 2020

Document Amendment History

Revision	Originator of change	Date of change	Change description
V 1.1	Becky Scott LDSM	June 2018	Updating policy in view of General Data Protection Registration (“GDPR”) and new Data Protection Act 2018 (“the Act”), and amendments to roles

1. Contents

2. Overview	4
2.1. What is Records Management?	4
2.2. What records does the Council keep?	4
2.3. The relevant legislation.....	4
3. Purpose.....	5
4. Scope	5
4.1. Accuracy of personal records and data	6
4.2. Access to records (Statutory public access).....	6
4.3. Standards for managing electronic records and email	7
4.4. Retention and Disposal Policy.....	7
4.5. Corporate Records Destruction Procedure	8
5. Policy Compliance.....	8
5.1. Compliance Measurement.....	8
5.2. Non-Compliance.....	8
5.3. Policy Review	9
6. Related Standards, Policies, and Processes	9
7. Definitions	9

2. Overview

2.1. What is Records Management?

Records management is the practice of maintaining records from the time they are created through to their eventual disposal. This may include the classifying, storing, securing and destruction (or in some cases, archival preservation) of records.

Records management is about controlling records within a comprehensive regime made up of policies, procedures, systems, processes and behaviours. Together they make sure that reliable evidence of actions and decisions is kept and remains available for reference and use when needed, and that the Council benefits from effective management of one of its key assets, its records.

Section 46 of the Freedom of Information Act 2000 (Code of Practice on Records Management) (“the Code”) defines a record as:

“Information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business”.

Records can be in any format. As the Code says:

“The code applies to all records irrespective of the technology used to create and store them or the type of information they contain. It includes, therefore, not only paper files series and digital records management systems but also business and information systems (for example case management, finance, and geographical information systems) and the contents of websites.”

2.2. What records does the Council keep?

At City of Lincoln Council (“the Council”), we keep records about the way in which we carry out our statutory and other functions, the people to whom we provide services and others with whom we deal, our policies, procedures and decisions about everything that matters to us and that staff need to do their jobs. Our staff keep these records as part of their daily work.

2.3. The relevant legislation

When developing policies, procedures and guidance involving the management of records the Council will comply with the following legislation, regulations and guidance and any other legislation as appropriate:

- Data Protection Act 2018
- The Freedom of Information Act 2000
- Section 46 of The Freedom of Information Act 2000 (Code of Practice on Records Management)
- Re-use of Public Sector Information Regulations 2015
- Financial Regulations

- Employment legislation
- Health and safety legislation

3. Purpose

The Council is committed to improve the way in which it creates, maintains, uses and destroys information and records. The purpose of this Policy is to set out the framework of rules and principles we will put in place to achieve this.

4. Scope

Development of records management procedures and practices are the responsibility of the Senior Information Risk Owner (SIRO), Data Protection Officer and the Freedom of Information Officer/the Legal and Democratic Services Manager.

All employees and Elected Members are responsible for the records they hold on behalf of the Council. They must follow this policy and all procedures, guidance, including the Retention and Disposal Policy.

All records created by Council employees and Elected Members will remain the property of the Council.

The creation, maintenance and destruction of records are the responsibility of the department providing the service. Each department must manage records in accordance with this Policy and all associated policies and procedures. It is essential records are stored securely and the Asset Register is updated, so that the location of files are known by staff at all times Policy

We will make sure the following rules and principles are embedded in all our service provision and processes:

- We will manage records in appropriate management systems and organise them accordingly (for example alphabetically, numerically, in date order, etc). Where appropriate, reference numbers and/or version control will be applied to help with locating records in the future, and for identifying records stored prior to destruction.
- We will maintain the Retention and Disposal Policy to make sure that records are kept for a period defined by relevant legislation and regulations before they are destroyed.
- We will provide mandatory training for employees on the importance of managing records effectively. Elected members will also be trained.
- We will make sure that policies, procedure and guidance are used in conjunction with the Council's the Retention and Disposal Policy.
- Audits will be carried out to monitor compliance with policy, procedure and guidance for safe and legal management of records.

4.1. Accuracy of personal records and data

The Council will make sure that all information is processed in accordance with the DPA. The Council's Data Protection Policy explains how employees are expected to comply with the Act when creating and maintaining records on behalf of the Council.

All records must be accurate, up to date and not excessive. Any corrections, amendments or additions to a record are to be made in accordance with departmental procedures and a record of changes retained for audit purposes.

4.2. Access to records (Statutory public access)

Subject Access Requests

The DPA gives individuals the right to access their personal information held by the Council. Policy, procedure and guidance can be found in the Council's Data Protection Policy and related staff guidance. This can be found on the Council's intranet.

Freedom of Information

The Freedom of Information Act gives the people a right to know what decisions are taken on their behalf by the Council on how services are run. The Council has published a Publication Scheme which shows what information can already be accessed. Any information which is not detailed in the Publication Scheme can be requested under the Freedom of Information Act although there may be exceptions to this where statutory exemptions apply.

Further guidance and contact information can be found in the Council's Freedom of Information and Environmental Information Regulations Policy and related staff guidance. This can be found on the Council's intranet.

Environmental Information Regulations

The Government has issued regulations to local Government which make it easy for people to access information about the state of the elements of the environment (air, atmosphere, water, soil, landscape, natural sites and ecology, biological diversity, and genetically modified organisms). Some information related to this is contained within the Council's Publication Scheme.

Further guidance and contact information can be found in the Council's Freedom of Information and Environmental Information Regulations Policy and related staff guidance. This can be found on the Council's intranet Standards for the storage of paper records

The Council will make sure records are protected from damaging elements such as water, light, temperature, humidity, fire and infestation.

The security of the information will also be protected by keeping storage units and rooms locked when not in use, where possible. Access to keys will be restricted to the responsible service area employees.

4.3. Standards for managing electronic records and email

Records will be managed in line with the Council's Retention and Disposal Policy and destruction and offsite storage Procedures which can be found on the Council's intranet.

Regular housekeeping is essential to make sure stored records are kept for the appropriate length of time in line with retention and disposal schedules. Records which form part of a service must be saved into the relevant system or shared work areas.

The Information Security Policy has further information on appropriate management of electronic records and email and is available on the Council's intranet or on request from from the Freedom of Information Officer/the Legal and Democratic Services Manager.

4.4. Retention and Disposal Policy

The Council's Retention and Disposal Policy identify the types of records held and length of time each document or electronic record must be retained, and when it should be destroyed. In some cases records are retained permanently.

Directorates are consulted on the types of records they hold and the appropriate length of time set for retention of those records are agreed. Requests can be made to change retention periods but there must be a valid business reason and agreement from the Data Protection Officer or the Freedom of Information Officer/the Legal and Democratic Services Manager or a member of the Legal Services Team. Some retention periods are governed by statutory legislation so it is important retention periods are applied correctly when deciding how long to keep or destroy a record.

All records have different retention periods, for example the destruction date may be from last involvement (closed record/last action entry) or from date of birth. This must be checked on the corporate retention and disposal schedules.

The Retention and Disposal Policy can be found on the Council's intranet Offsite Storage Procedure and Guidance

The Council is required to keep records for specified periods of time after involvements have ended. The length of time for keeping closed records varies dependent upon the nature of the involvement the Council had with the customer.

The retention period for each type of record is specified in the Council's Retention and Disposal Policy.

The Offsite storage procedure and guidance contains guidance in relation to the processes for preparing records prior to sending offsite and for retrieving closed records.

4.5. Corporate Records Destruction Procedure

The Council has a statutory duty under the DPA to make sure records relating to living individuals are not kept for an excessive amount of time. Where records exceed the retention period these must be destroyed unless there is a valid and legal reason for retaining.

If the responsible Directorate/department has a business need to retain information after the destruction date set, the Data Protection Officer or Freedom of Information Officer/the Legal and Democratic Services Manager or a member of the Legal Services Team must be notified and an agreement reached to change. Policy Compliance

4.6. Compliance Measurement

The Council will ensure compliance with this Policy by regularly reviewing organisational and technological processes to ensure compliance with Section 46 of the Freedom of Information Act 2000 (Code of Practice on Records Management) and all other relevant legislation including the DPA.

Where there are particular compliance measurements required by the DPA and the Freedom of Information Act 2000 and Environmental Information Regulations 2004 these are detailed in the Council's relevant Policies.

All policies relating to Records Management will be subject to scrutiny by the Policy Scrutiny Committee and/or the Audit Committee.

4.7. Non-Compliance

Non-compliance with this Policy could have a significant effect on the efficient operation of the Council and may result in prosecution, financial loss and damage to Council's reputation and ability to provide necessary services to our customers.

If any user is found to have breached this Policy, they may be subject to the Council's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

The Council encourages the notification of Data Protection breaches by staff in accordance with the Data Protection Breach Management Policy at the earliest opportunity. Notification will also be taken into account in any resulting disciplinary investigation, where the individual/s concerned have assisted in the containment of the breach.

If you do not understand the implications of this Policy or how it may apply to you, seek advice from the Data Protection Officer and the Freedom of Information Officer/the Legal and Democratic Services Manager or a member of the Legal Services Team.

4.8. Policy Review

This Policy will be reviewed every two years and updated in the interim as required.

5. Related Standards, Policies, and Processes

- Information Governance Policy
- Legal Responsibilities Policy
- Information Sharing Policy
- Data Quality Policy
- Data Protection Breach Management Policy
- Freedom of Information Policy & Environmental Information Regulations Policy
- Data Protection Policy
- Information Security Policy
- Retention and Disposal Policy

6. Definitions

Asset Register	The detailed breakdown of all records and information held by the Council and signed off by the Information Asset Owner. This includes details of location, format, security access restrictions, data flows and assesses any risks to assets.
Records management	The discipline and professional function of managing records in order to meet organisational needs, business efficiency and legal and financial accountability.
Information Asset Owner	<p>The IAO was established by the Security Policy Framework. Their role is to protect and manage information held in the Council, and ensure that its value to the organisation is recognised. They are also responsible for promoting and fostering a culture of security of data within their teams and wider organisations.</p> <p>Information Asset Owners within the Council are all Service Managers and where appropriate Team Leaders.</p>

SIRO	<p>Senior Information Risk Owner.</p> <p>Leads the organisation's response on information risk and is responsible for ensuring organisation's information is managed securely. They are often a senior individual within the organisation and are a main point of contact for IAO's.</p>
Retention	<p>Means the length of time for which records are to be kept. Thus it normally represents and will be expressed as a disposal period.</p>
Disposal	<p>In this context does not just mean destruction: it embraces any action taken (or yet to be taken) to determine the fate of records including transfer to a permanent archive.</p>
Information security	<p>The policies, procedures and practices required to maintain and provide assurance of the confidentiality, integrity and availability of information.</p>
Compliance	<p>In the context of Information Management, compliance relates to the Council's need to operate in accordance with the existing legislation, regulations and best practices.</p>