Leicester
City Council

Digital, Data and Technology
Policies and Guidance

Information Management Policy

29th September 2022

Document Version: 2.2
Review Date: September 2023

Owner: Head of IT Operations, Digital, Data and Technology (DDaT)

1.0 Introduction

The aim of this policy is to manage information held by the Council efficiently and effectively.

Effective Information Management makes service delivery more efficient, supports transparency, collaboration across departments, and informed decision making in authority operations, and preserves historically valuable information.

The introduction of standardised Information Management systems will enable the Council to deliver reductions in bureaucracy and raise the performance of all key business processes.

2.0 Scope

Information and records are corporate resources owned by the Council. All information and records must be managed in accordance with stated policy and associated documents.

This policy applies to all information and records held by the Council, regardless of format and all information systems used to create and store records.

This policy applies to all Council staff, collaborative partners and contractors with access to Council records or information systems.

3.0 Key Definitions

Information Management describes the means by which the Council plans, organises, creates, controls, and disseminates information. It is an approach that allows the Council to maximise the value of information to support service delivery.

A record is any recorded information that captures and provides evidence for the Council's business activities, decisions and transactions.

Records management is the practice of maintaining these records in physical form (paperwork) and/or electronic form (electronic documents, databases, e-mail, scanned documents, etc.) from the time they are created until their disposal.

4.0 Policy Statement

Information is a valuable asset that the Council must manage as a public trust on behalf of the City of Leicester.

In order to improve the management of information we will;

- Ensure **information security** and **safeguard** vital data,
- **Create** and **capture quality information** to support better decision making,
- **Review** and **dispose** information that is no longer required and reduce operational costs,
- **Effective data** management to **reduce duplication** of information and improve service delivery,
- **Conform** to all **legal** and **statutory** requirements,

- **Collaborate** and **share** information more effectively with partners to improve the wellbeing of citizens,
- **Improve** staff **skills** and competencies.

5.0 Key Governance Bodies

The purpose of the Corporate Information Group (CIG) is to:

- Provide leadership and strategic governance across the Council on Information Governance, Information Management and Information Security (collectively known as Information Assurance).

The CIG's primary functions and objectives are:

- To provide a forum to bring together all strands of Information Assurance across the Council to enable a joined up and coherent approach.
- To provide consistent advice on information assurance matters to The Council's decision makers so that they can make informed decisions on resource attribution and prioritisation.
- To maintain a forward look on innovation and developments and ensure these are influencing strategic direction where appropriate.
- To develop, share and showcase best practice developments to encourage adoption.

6.0 Key Information Management Principles

The aims of this policy will be achieved by implementing work to establish the following Information Management principles:

We will make information **accessible** to others (who need and are authorised to access it).

We will treat information as a **valuable resource**.

We are **all responsible** for our information.

We will maintain **quality** by **keeping records** of what we do.

We will provide staff with **key information management skills**.

Our information will **comply** with **regulations** and **legal** requirements.

7.0 Policy Requirements

It is essential that the Information Management principles are developed into standards, guides and tools that support all business processes. These standards, guides and tools are highlighted in the Information Management Strategy.

8.0 Roles and Responsibilities

This policy establishes responsibilities for all staff which include;

Senior Information Risk Officer (SIRO); The SIRO is responsible for setting strategic direction and ensuring that policies and processes are in place for the safe management of information. The SIRO is supported in this role by CMT, Strategic Directors and Service Directors and the CIG.

Information Asset Owners (IAOs); An IAO is typically a Director or Head of Service and has overall responsibility for data held with systems relevant to their respective departments, divisions and services. The IAOs are responsible for information assets within their business unit as they are best able to understand how information is held, used and shared and address risks to the information. IAOs are responsible for ensuring appropriate information management practices are in place for their information assets (electronic and paper). They will ensure appropriate backup arrangements are in place for electronic records (including restoration of backups and disaster recovery if electronic records are damaged). It is the responsibility of the IAO to ensure any changes to their information is updated on the information asset register and also ensure any relevant entries on the corporate retention schedule are reviewed periodically.

Data Stewards; Data stewards are nominated by an IAO and act as delegates to them in ensuring that information assets are managed in line with appropriate information management practices as directed by the IAO. They have a responsibility to carry out day-to-day information management tasks and ensure data quality is maintained to the highest levels possible. Specific responsibilities will be unique to the area and the amount of responsibility delegated to them by the IAO.

All Staff; All employees are responsible for applying Information Management principles, standards and practices in the performance of their duties; and documenting their activities and decisions that produce business information.

Team Managers; Responsibilities of team managers accountable for implementing this policy include ensuring that the effectiveness of Information Management policy implementations are periodically assessed and ensuring implementation of this policy and associated guidance.

Heads of Service; Responsibilities of heads of service include promoting a culture that values information and its effective management: and allocating appropriate resources to support Information Management.

Corporate Information Group; acts as an advisory group to the following decision makers: The City Mayor and the Executive, The SIRO, CMT, Strategic Directors and Service Directors. The CIG is responsible for approving this policy.

Digital, Data and Technology (DDaT); DDaT are responsible for providing and maintaining the secure infrastructure to enable information users to have access to information they require to deliver their services.

Where information is stored, managed or hosted elsewhere on behalf of the Council, Digital, Data and Technology when required will make appropriate contractual arrangements to ensure the safe keeping, transfer, appropriate use, disposal and/or return of information at the end of the contract.

Enterprise Content Management; Develops and implements Enterprise Content Management programmes, policies and classification systems to meet the requirements of the Council's corporate objectives, in consultation with internal and external stakeholders. ECM also establishes, manages and monitors contracts for outsourced information related services, including scanning.

9.0 Performance Management

Information Management Key Performance Indicators will be introduced and monitored to provide evidence of departmental performance.

The Corporate Information Group will monitor the performance of this policy.

10.0 Legislation Compliance Statement

This policy has been drafted in accordance with all relevant legislation. In addition, this policy will establish a framework for compliance with a range of quality standards, including ISO Information Management 15489-1:2016.

Further Information and links

InterFace Pages:

Information Governance

IT Security

Information Management

DDaT Policies and Guidelines

Useful training resources:

Leicester Learning Pool

Related Documents:

DDaT Security Policy - DDaT Policies and Guidelines

DDaT Acceptable Use Policy AUP - DDaT Policies and Guidelines

Record Retention Schedule

Data Quality Standards