London Borough of Enfield

Information Management Strategy
INFORMATION MANAGEMENT STRATEGY

1. Introduction
This strategy sets out Enfield Council’s aims and priorities for the way it manages information.

Enfield’s three aims of:

- Good homes in well-connected neighbourhoods
- Sustain strong and healthy communities
- Build our economy to create a thriving place

all rely on the effective use of information if we are to ensure we use our resources effectively to meet the needs of our community, champion our needs at a national level, be an open and accountable organisation that works in partnership with others.

This is supplemented by our organisational principles of:

- Communicate with you
- Work with you
- Work smartly for you

Breaking down barriers to collaborative working, effective decision making and understanding of our community is critical to delivering these values.

This strategy, its principles, goals and actions are aimed at delivering these outcomes. It is an overarching document which supports and is supported by a number of policies and procedures as set out in sections 6 and 7 below.

2. Vision
_Enfield Council will create an environment where information is valued as a corporate asset. Information is collected, stored, used, shared and disposed of in a way that ensures the integrity, sensitivity and security of the asset whilst giving staff and councillors the information they need to be empowered to deliver the Council’s aims and objectives. We will be open and accountable with our data whilst ensuring that information is suitably protected and processed fairly._

3. Scope of this strategy
This strategy applies to all staff, temporary workers, councillors, contractors, agents and representatives working for or on behalf of the Council.
It covers all information created or held by the Council in whatever format (paper, electronic, email, microfiche, CDs, film) and wherever it is stored.

**Definition of information management**
Information management is the function of managing the organisation’s information resources. It includes creating, capturing, registering, classifying, indexing, storing, sharing, retrieving, providing, using and disposing of information assets in the most efficient and effective way. The three key elements in effective information management are confidentiality, integrity and availability.

It is important to understand the information lifecycle, as the strategy covers managing information; from initial creation, through reuse and publishing, and finally to disposal or permanent archive.

![Information management lifecycle diagram](image)

Information is received or created, and will be used and re-used many times over, by users sharing and collaborating to amend and create different views and analysis. To use information efficiently it must be stored once and be accessible within a controlled environment.

4. **The Information Principles**

Information is a key asset of the organisation, and we will be guided by following the principles that information is:

- held only once and duplicated only for backup
- able to be combined with other information to aid decision making
- owned, managed and kept no longer than necessary
- accurate, relevant and fit for purpose
- kept securely
- readily available to all when they need it, unless there are good reasons to restrict access
5. Our goals

The principles will be achieved by delivering the goals and measures below.

Information security and integrity
- Information is processed and stored securely to maintain confidentiality, integrity, legality, availability and ensure business continuity.
- We will share relevant information across the authority and, where appropriate, with partners and contracted service providers through information sharing protocols to enhance the quality and targeting of local services.
- Our IT infrastructure and business processes support these principles to avoid duplication of effort and ensure that data and systems are protected from unauthorised or accidental modification.
- Management information is available to staff, managers, councillors and partners in a timely way that is easy to understand and informs effective decision making.

Records management policy
- Information is captured, stored and created digitally as a default with only archive materials in paper format.
- Information is up-to-date, accurate and consistent across the organisation.
- Information is owned, classified and indexed based on national standards at the point of creation.
- The organisation has a culture of controlled disposal of unnecessary information and preservation of information of merit and importance in line with the Council’s Retention Scheme.

Confidentiality
- Personal and sensitive personal information will be collected, stored and processed in line with current legislation.
- Staff and councillors understand their information responsibilities, respect the privacy of personal information and are competent in using information effectively.

Transparency and availability
- The council is recognised by the public as a responsive and transparent organisation, with the majority of information requests and queries resolved at the first point of contact.
• Information is presented in an accessible way that is easy to understand and takes into account the needs of people with disabilities
• The organisation has a culture of openness, to share information with staff, councillors, partners and the public wherever possible, while respecting that personal information needs to be restricted
• Individuals will be provided with access to information held about them and be advised for what purposes it is being processed

**Governance**

• Staff will be provided with information governance training to ensure they have a clear understanding of their own responsibilities and the Council’s duties as a Data Controller
• We will monitor the delivery of these goals through the governance framework set out in section 8
• Information security incidents will be reported and analysed to ensure lessons are learnt
6. Where does this strategy sit?

7. Related policies and legislation

Some of the other policies and documents linked to this strategy are:

- Acceptable Use Policy
- Access Control Policy
- Business Continuity plan
- Business plans
- Corporate Risk Strategy
- Data Protection Policy
- Employee Code of Conduct
- Freedom of Information Policy
- ICT strategy
- Information Classification and Handling Policy
- Records Management Policy (including retention scheme)
- Register of Information sharing protocols
- Security Incident Reporting Procedure
- Third party access and management policy
Regulations and standards applicable to this policy include:

- Data Protection Act 2018 (included the Applied General Data Protection Regulation EU679/2016)
- Freedom of Information Act 2000
- Section 224 of Local Government Act 1972
- ISO 15489 International Standard for Record Management
- ISO 27001
- E-Government Interoperability and Metadata Frameworks
- UK Gov Minimum Cybersecurity standards
- PCI-DSS requirements
- PSN Code of Connection requirements
- Access to Health Record Act 1990
- BS 10008 Evidential weight and legal admissibility of electronically stored information (ESI)
- Common Law Duty of Confidence
- Human Rights Act (Article 8)
- Caldicott Principles

8. Governance framework and responsibilities

Senior roles:
- Senior information risk owner (SIRO) is the Director of Law and Governance
- Information Governance lead officer is the Chair of the Information Governance Board, currently Head of Legal
- The two Caldicott Guardians are Assistant Director Safeguarding for children and Joint Chief Commissioning Officer for adults
- Lead member for information governance

Key roles:
- Data Protection Officer
- IT Security Manager is the Information Security Officer for the Council
- Freedom of Information Officer
- Departmental Data Co-ordinators
- Chairman of the Access to Information Working Group
- Head of Corporate Policy and Performance – lead officer for data quality

Responsibilities:
- Whilst the Council is nominated as a Data Controller, ultimate accountability lies with the Chief Executive and the Senior Information Risk Owner
- Executive Management Team (EMT) is responsible for ensuring sufficient resources are provided, designating departmental data co-
ordinators and for monitoring compliance within their department, taking corrective action as necessary

- Information Governance Board (IGB) monitors performance, oversees, reports, drafts policies and makes recommendations to EMT on strategic information governance issues

- The Data Protection Officer (DPO) is responsible for the Council’s registration with the Information Commissioner’s Office and reviewing compliance with current legislation. This role liaises with the Information Commissioner’s office in dealing with complaints and reports to IGB on incident management. Note that individual data owners are responsible for compliance and consulting with the DPO on all decisions relating to personal data; by law the DPO must be independent and not take decisions in this area.

- The Records Manager will ensure effective compliance with the records management policy and retention scheme

- Information Asset/System owners are accountable for ensuring compliance with legislation and council policies, and consulting with the DPO and reporting/recording disagreement with their advice where not followed.

- Departmental Data Co-ordinators will be responsible for ensuring that staff and contractor know of their responsibilities, understand and follow procedures for handling, releasing and disposing of information and confirm that personal information complies with the DPA. Each attends the Information Governance Board.

- A freedom of information lead officer and Access to Information Working Group will ensure effective organisational procedures are in place to support Freedom of Information and Subject Access Requests and will report to the IGB.

- Staff and councillors are required to be aware of and comply with the relevant policies and legislation, undertake training as required of them and report information governance issues/incidents using the set procedures

- Information Governance updates and issues will be reported to the Council’s Audit Committee at least annually

9. Training and education

Enfield Council will provide staff and councillors with the necessary information, procedures and training required for them to undertake their roles and their responsibilities contained in this policy effectively.
10. Action plan

IGB will maintain an action plan and report on it annually to EMT.

11. Monitoring and review

This strategy and action plan will be reviewed by the Information Governance Board and reported to the Executive Management Board annually.