North West Leicestershire District Council

INFORMATION MANAGEMENT POLICY

Version Control

Version No.	Author	Date	Update Information
V1.0	Lynn Wyeth	20.11.2015	Original Draft
V1.1	Lynn Wyeth	04.12.2015	Amendments by NWLDC incorporated
V1.2	Lee Mansfield	15.12.2015	Amendment made following CLT decision - SIRO
V1.3	Lee Mansfield	02.02.2016	To reference legal as location of the IM team
V1.4	Sabrina Doherty	23.02.2017	Changes made to team structures, functions, roles and responsibilities
V1.5	Andrew Hickling / Louis Sebastian	09.05.2018	Changes made to team structures, functions, roles and responsibilities
V1.6	Nicola Taylor / Mackenzie Keatley	01.07.2020	Change made to team structures, roles and responsibilities, training and support, legislation update

June 2020

INFORMATION MANAGEMENT POLICY

POLICY STATEMENT

"Information is a vital corporate asset of the Council which is of extremely high value. North West Leicestershire District Council is committed to ensuring that information is efficiently managed and that appropriate policies, procedures, management accountability and structures provide a robust governance framework for information management."

1. INTRODUCTION

1.1 The key areas of Information Management are:

- Records Management;
- Information Risk;
- Information Security;
- Environmental Information Regulations 2004;
- Freedom of Information Act 2000;
- Data Protection Act 2018;
- General Data Protection Regulations;
- Local Government Transparency Code 2015;
- Privacy and Electronic Communication Regulations;
- Public Services Network Code of Connection;
- Payment Card Industry Security Standards;
- Confidentiality.

1.2 This policy is part of a set of information management policies and procedures that support the delivery of an Information Management framework, and should be read in conjunction with these associated documents, listed at section 4.

2. PURPOSE OF THE POLICY

2.1 This Information Management policy provides an overview of the Councils approach to information management, a guide to the procedures in use, and details about the management structures within the organisation.

2.2 This policy enables the Council to ensure that all information is dealt with legally, fairly, securely, efficiently, and effectively.

2.3 This policy ensures that the provisions of the Freedom of Information Act 2000 (FOI), the Environmental Information Regulations 2004 (EIRs), the Data Protection Act 2018 (DPA), the General Data Protection Regulation (GDPR) and the Public Services Network Code (PSN CoCo) are complied with.

3. SCOPE OF THIS POLICY

3.1 This policy, framework and supporting policies apply to:

- all information systems within the organisation (both electronic and paper based);
- all data, information, and records owned by the Council, but also including those held by contractors or partner organisations on behalf of, or as a result of their relationship with, the Council);

- any information that is owned by other organisations, but may be accessed and used by Council employees;
- information in whatever storage format and however transmitted (i.e., paper, voice, photo, video, audio or any digital format. It will also cover formats that are developed and used in the future.);
- all employees of the Council, Council members, temporary workers, volunteers, student placements, etc;
- the employees of any other organisations having access to Council information, for example, auditors, contractors, and other partner agencies where there is no specific information sharing protocol in place,

3.2 The procedures outlined in this Policy are in addition to the Council's complaints procedures and other statutory reporting procedures applying to some divisions.

3.3 This Policy has been discussed with the relevant trade unions and has their support.

4. PROCEDURES AND GUIDANCE

4.1 This Information Management Policy will be strengthened by other associated Council policies / procedures / material including but not limited to:

- ICT Security Policy;
- Request for Information Procedure;
- Security Incident Procedure;
- Records Management Procedure;
- Information Sharing Procedure;
- Whistleblowing Policy;
- RIPA Policy;
- Anti-Money Laundering Policy;
- Employment Practices Code - Information Commissioner's Office.

5. PRINCIPLES OF INFORMATION MANAGEMENT

5.1 The Council understands the need for an appropriate balance between openness and confidentiality in the management and use of information. The Council also understands the need to share information with others in a controlled manner.

5.2 To maximise the value of organisational assets the Council will endeavour to ensure that data is:

- held securely and confidentially;
- obtained fairly and lawfully;
- recorded accurately and reliably;
- used effectively and ethically;
- shared and disclosed appropriately and lawfully;

5.3 To protect the organisation's information assets from all threats, whether internal or external, deliberate or accidental, the Council will ensure:

- information will be protected against unauthorised access;
- confidentiality of information will be assured;
- integrity of information will be maintained;
- information will be supported by the highest quality data;

- regulatory and legislative requirements will be met;
- business continuity plans will be produced, maintained and tested;
- information security training will be mandatory for all staff;
- all breaches of information security, actual or suspected, will be reported via the Security Incident Procedure and investigated by the Data Protection Officer or Information Management Officer;
- significant breaches will be handled with support from Human Resources and/or ICT Manager and/or Legal Services;

6. ROLES AND RESPONSIBILITIES

6.1 Information Asset Owners

6.1.1 Information Asset Owners (IAOs) are Heads of Service who are the nominated owners for one or more identified information assets within the Council. Their role is to understand what information is held, added, removed, how information is moved and who has access and why.

6.1.2 Information Asset Owners will:

- know what information comprises or is associated with the asset, and understand the nature and justification of information that flows to and from the asset;
- know who has access to the asset, whether system or information, why access is required, and ensures access is monitored and compliant with policy;
- understand and address risks to the asset, providing assurance to the Senior Information Risk Owner;
- ensure there is a legal basis for processing data and for any disclosures made;
- refer queries about any of the above to the Information Governance Team.

6.2 Senior Information Risk Owner

6.2.1 From 1 July 2016 the Head of Legal and Commercial Services will become the SIRO.

The SIRO will report to the CLT on all matters relating to Information Management. The SIRO is an executive who is familiar with and takes ownership of the organisation's information risk policy, and acts as advocate for information risk.

6.3 Data Protection Officer

6.3.1 As of the 4 November 2018 the Council appointed a Data Protection Officer.

Under GDPR it is mandatory that a public authority appoint a Data Protection Officer (DPO).

The DPO's tasks are defined in Article 39 of the GDPR.

The DPO Information Management responsibilities include:

- implementing information management procedures and processes for the organisation;
- raising awareness about information management to all staff;
- ensuring that training is provided annually and is completed by all staff;

- co-ordinating the activities of any other staff given responsibilities for data protection, confidentiality, information quality, records management and Freedom of Information;
- conducting internal audits to ensure compliance on an ad-hoc basis;
- ensures the Council is responsible for the continued integrity of datasets and maintains and enforces applications of policies and standards;
- to co-operate with the supervisory authority (ICO).

6.4 Information Governance

6.4.1 Information management is co-ordinated and managed by the Information Governance Team. The Team will:

- assist the Senior Information Risk Owner in the implementation of their key responsibilities and any other matters as deemed appropriate and necessary;
- maintain an awareness of information management issues within the Council;
- review and update the information management policy in line with local and national requirements;
- review and audit all procedures relating to this policy where appropriate on an ad-hoc basis;
- ensure that line managers are aware of the requirements of the policy.

6.5 ICT Team Manager

6.5.1 The ICT Team Manager is responsible for:

- the formulation and implementation of ICT related policies and the creation of supporting procedures;
- developing, implementing and managing robust ICT security arrangements in line with best industry practice, legislation, and statutory requirements;
- effective management and security of the Council's ICT infrastructure and equipment;
- developing and implementing a robust IT Disaster Recovery Plan;
- ensuring that ICT security requirements for the Council are met;
- ensuring the maintenance of all firewalls, secure access servers and similar equipment are in place at all times.

6.6 Head of Service / Team Managers

6.6.1 Heads of Service / Team Managers will take responsibility for ensuring that the Information Management Policy is implemented within their team. All managers will ensure that:

- the requirements of the information management policy framework are met and its supporting policies and guidance are built into local procedures;
- there is compliance with all relevant information management policies within their area of responsibility;
- information management issues are identified and resolved whenever there are changes to services or procedures;
- their staff are properly supported to meet the requirements of information management and security policies and procedures, by ensuring that they are aware of:
  - the policies and procedures that apply to their work area;
  - their responsibility for the information that they use;

- where to get advice on security issues and how to report suspected security incidents.

6.7 Staff

6.7.1 It is the responsibility of each employee to adhere to this policy. Staff will receive instruction and direction regarding the policy from a number of sources, including:

- policy / strategy and procedure manuals;
- their line manager;
- the legal team;
- specific training courses;
- other communication methods, for example, team meetings; and staff intranet.

6.7.2 All staff (whether permanent, temporary, voluntary or on any type of placement / training scheme) and members must make sure that they use the Council's IT systems appropriately and adhere to the relevant ICT Policies of the Council. All members of staff are responsible for:

- ensuring that they comply with all information management policies and information security policies and procedures that are relevant to their service;
- seeking further advice if they are uncertain how to proceed;
- reporting suspected information security incidents.

6.7.3 Staff awareness is a key issue in achieving compliance with Information Management policies. Accordingly there will be:

- mandatory base line training in key information management competencies for all staff;
- additional support for all employees routinely handling 'personal data' as defined by the Data Protection Act 2018;
- all information management policies and procedures available on the intranet;
- staff with specialist knowledge available to advise across the full range of information management areas;
- communication and updates will be provided to staff regularly;
- services are encouraged to have an Information Champion to represent their service. Key messages, training and support are provided to the Information Champions who feed this back to their service. Information Champions can raise issues with the group to identify and remedy problems.

7. MAIN THEMES

7.1 Openness

7.1.1 Non-confidential information which the Council hold will be made available to the public through the Councils website wherever feasible and appropriate.

7.2 Legal Compliance

7.2.1 The main legislation applying to information management is the Data Protection Act 2018 and the Freedom of Information Act 2000. The Council will establish and maintain procedures to ensure compliance with the Data Protection Act 2018, the Freedom of Information Act 2000, the Environmental Information Regulations 2004, and the Humans Rights Act 1998.

7.3 Information Security

7.3.1 Information security is concerned with the confidentiality, integrity, and availability of information in any format, and the Council must comply with the requirements of the Public Services Network.

7.4 Information and Records Management

7.4.1 To ensure that information and records are effectively managed, and that the Council can meet its information management objectives, there will be a Records Management Policy that sets out the Council's standards for handling information during each phase of the information lifecycle.

7.5 Information Quality Assurance

7.5.1 The Council will undertake or commission regular assessments and audits of its information quality and records management arrangements.

7.5.2 Managers are expected to take ownership of, and seek to improve, the quality of data within their services. Training and awareness-raising sessions appropriate to staff groups will be provided.

7.6 Partnerships and Information Sharing

7.6.1 Any sharing of personal or confidential information with partner agencies or involving individual large transfers of such information will be the subject of a written Information Sharing Agreement (ISA). This will set out the expected process, the standards of security and information handling.

8. RISK

8.1 The Council must ensure it operates within a robust information management framework to reduce the risk of threats such as potential litigation, breach of legislation, or enforcement action from the ICO for failure to respond to information requests adequately.

9. TRAINING

9.1 Appropriate training will be mandatory for all staff.

9.2 All staff will be made aware of their obligations for information management through effective communication programmes.

9.3 Each new employee will be made aware of their obligations for information management during an induction-training programme and will be required to undergo mandatory data protection training before they can pass their probation period.

9.4 Training requirements will be reviewed annually to ensure that staff are adequately trained.

10. COMPLIANCE

10.1 Failure to observe the standards set out in this policy may be regarded as serious and any breach may render an employee liable to action under the Council's Disciplinary Procedure, which may include dismissal.

11. FEES AND CHARGES

11.1 The Council aims to provide as much information free of charge on the website for customers to download or view at home. The Council may charge in accordance with the charges set out in legislation or statutory guidance and for the cost of disbursements such as photocopying and postage.

12. COMPLAINTS

12.1 Any person who is unhappy with the way in which the Council has dealt with their request for information, or how their personal data has been handled, may ask for the matter to be reviewed. All complaints should be in writing to:

- DPO@NWLeicestershire.gov.uk (personal data requests)
- FOI@NWLeicestershire.gov.uk (non-personal information request)
- Data Protection Officer
  North West Leicestershire District Council
  Whitwick Road
  Coalville
  Leicestershire
  LE67 3FJ

12.2 Should the requester / complainant still be unhappy with the outcome of this review they have the right to pursue their complaint to the Data Protection Officer for a formal review. Following the Internal Review, the requester can contact the Information Commissioners Office (ICO, www.ico.org.uk) by writing to:

- accessicoinformation@ico.org.uk
- Information Commissioner's Office
  Wycliffe House
  Water Lane
  Wilmslow
  Cheshire
  SK9 5AF

13. EQUALITIES IMPACT ASSESSMENT

13.1 Equality and diversity issues have been considered in respect of this policy and it has been assessed that a full Equality Impact Assessment is not required as there will be no adverse impact on any particular group.

14. REVIEW OF POLICY

14.1 This policy will be reviewed as deemed appropriate, especially in light of any legislative changes, but no less frequently than every 12 months.

14.2 Policy review will be undertaken by the Information Governance Team.