Nottinghamshire County Council

Information Management and Data Quality Policy

Context

1. The purpose of this policy is to maximise the effectiveness of Nottinghamshire County Council by managing data, information and records as strategic corporate assets and ensure compliance with relevant legislation.

2. Effective data and information management (IM) makes service delivery more efficient, and supports transparency, collaboration across departments, and informed decision making in Council operations. It also preserves historically valuable information and records.

3. The introduction of standardised IM systems and data quality will enable the Council to deliver reductions in bureaucracy and raise the performance of all key business processes.

Scope of this policy

4. Information management - includes the management of information, data, documents and records

5. Data, information and records are corporate resources owned by the Council. All data, information, documents and records must be managed in accordance with this policy and associated documents.

6. This policy applies to all data, information and records held by the Council, regardless of format. This includes documents and records in electronic or digital form as well physical form (hardcopy).

7. This policy applies to all elected members, officers, volunteers, contractors and consultants. It will also be applied to data, information and records provided by the Council's partners.

Aim and Commitments

8. Information must be managed using sound processes. The aim of this policy is to create a framework for managing the Council's information, data and records. The Council therefore commits to the following :

    To be compliant with all relevant legislation;

The creation and capture of accurate business information, data and records;

To review and appropriately dispose of information, data and records that are no longer required;

To ensure information security;

To conform to all legal and statutory requirements;

To ensure that all staff have been made aware of their duty of care and appropriately trained in order to deliver the commitments of this policy;

To ensure accuracy of all information, records and data held by the Council;

To collect information once, where possible and utilise it appropriately to deliver a range of services;

To only collect information that is necessary for the delivery of services.

Responsibilities

9. This policy establishes responsibilities which include;

All officers, volunteers, contractors, consultants and agency staff are responsible for applying IM principles, standards, and practices in the performance of their duties.

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

Leadership and management teams; Responsibilities of management teams include promoting a culture that values information and its effective management; and allocating appropriate resources to support information management.

SIRO; the Senior Information Risk Owner is responsible for leading and fostering the organisational culture that values, protects and uses information for the public good. The SIRO also owns the overall information risk policy and risk assessment process.

Corporate leadership team; the corporate leadership team will be responsible for ensuring that this policy is supported at all levels within the Council.

Elected Members; Members of the Council are responsible for protecting the information and data which they have access to or are exposed to in the course of their County Council activities in accordance with the constitution, this policy, its supporting documents and relevant legislation.

Information manager; the information manager has specific roles and responsibilities related to the management of information, which include developing and promoting a framework for the management of information, including guidance, tools and best practices that support this policy; and for the provision of appropriate advice.

Information Governance Management Framework – this framework provides the reporting structure in respect of information management and governance activities within the departments as well as the supporting advisory and compliance structure.

ICT Services; are responsible for ensuring that information and data management facilities are appropriate; effective and secure in accordance with legislative and statutory requirements. This will include the undertaking, and documentation, of appropriate risk assessments in respect of system and database security. ICT services are also responsible for ensuring that ICT security policies are maintained and adhered to.

Internal Audit; The team will be responsible for ensuring that data quality meets the appropriate standard and that each audit undertaken has an element of challenge to ensure that information management and data quality are addressed in accordance with this policy and supporting documents.

Non-compliance with the policy

10. Appropriate training and support will be available to all employees so that they may be fully competent in managing and handling information, data and records. Any case of non – compliance with this policy may lead to disciplinary action under the current disciplinary procedure

11. Examples of deliberate non-compliance are:

Consistent disregard to data and information management improvement;

Disclosure of protectively marked, restricted, or confidential information to unauthorised sources;

Loss of data / information through negligence, carelessness or disregard of a clear duty of care;

Unauthorised use of data and/or sending defamatory information;

Creating, processing of use of any data known to be inaccurate, misleading or invalid particularly with external agencies or the public;

Use of data for illicit or illegal purposes which may include violation of any law or regulation or any reporting requirement of any law enforcement or government agency.

Legislation Compliance Statement

12. This policy along with other elements of the Council's information management policy framework has been drafted in accordance with all relevant legislation, including:

    Freedom of Information Act 2000;

    Data Protection Act 1998;

    Human Rights Act 1998;

    Environmental Information Regulations 2004.

13. In addition this policy will establish a framework for compliance with a range of quality standards, including BSI ISO Information Management 15489: 2001 and BS 10008 – 1: 2008

Associated Documents

14. This policy statement overarches a range of procedures and guidelines. These documents provide more detailed instruction and guidance in relation to the implementation of the principles outlined in this statement. These documents include:

    L1-IM-PS-003 – IM Strategy.

    L3-IM-CS-010 – IM Procedure & Standards.

    L3-IM-CS-033 – Vital Records Standard.

    L3-IM-CS-035 – Managing Electronic Documents & Records.

    L3-IM-CS-011 – IM Admissibility of Electronic Documents & Records.

15. This policy should also be read in conjunction with the Constitution and the Council's policies on

    The Data Protection Act.

The Freedom of Information Act.

The Environmental Information Regulations.

The Regulatory Investigation Powers Act.