Information Governance Strategy

April 2018

districtnk
100 flourishing communities
North Kesteven District Council

Alternative Formats

This document can be made available in large print, Braille, audio tape, electronic formats such as CD, or in a different language. Our website is ReadSpeaker enabled. For a copy please contact the Corporate Information Team at the Council using the following options:

Phone: 01529 414155 (main switchboard)

Fax: 01529 413956

Web: www.n-kesteven.gov.uk

Email: equality@n-kesteven.gov.uk

Corporate Information Manager
North Kesteven District Council
Kesteven Street
Sleaford
Lincolnshire
NG34 7EF

Information Governance Framework
Information Governance provides a framework for bringing together all of the requirements, standards and best practice that apply to the handling of information. It allows organisations and individuals to ensure that information is accurate, dealt with legally, securely, efficiently and in order to deliver the best possible care.

The Council is committed to preserving the confidentiality, integrity and availability of all its physical and electronic information systems and records in order to provide assurance that the organisation manages its information risks:
• So that the needs of service users and stakeholders are met;
• To establish confidence that arrangements involving sharing and exchange of information are legal and secure;
• To ensure that information security features are effective.

The need for a comprehensive information governance framework also arises from:
• Legal (legislation and common law), regulatory and contractual requirements;
• Corporate governance;
• Business and service delivery;
• Protecting the public purse;
• Business continuity requirements.

Information Governance Principles
Information is a key asset of the organisation. The following principles help guide the use of information, which will be:

- held only once
- 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
- personal information will only be accessible to those who need it in order to carry out their functions
- conforms to legal, regulatory and authority policies and standards.

The principles will be achieved by delivering the goals 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, with the objective of enhancing 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
- Information governance material is available to colleagues, managers, councillors and partners in a timely way that is easy to understand and informs effective decision making.

The Council should manage information as a corporate asset in a way that it is:

- Efficient – using and exploiting information to improve cost effectiveness,
- Effective – providing the information required – securely, quickly, easily, accurately, conveniently, consistently, and transparently

- Accessible – ensuring information can be easily accessed by and is appropriate to the needs of the various user communities within and beyond the Council; encouraging the capture of knowledge held by individuals that can be shared with others for the common good
- Compliant – storing the right things in the right place and following the right policies at the right time.

The outcomes achieved will be:

- Information Systems that support the council's key business needs
- Better informed decision making
- Employees spending more time using information rather than searching for it
- Efficiency savings: better use of accommodation, less paper, reduced duplication of information and process
- Compliance with Government standards
- Improved staff skills and competencies
- More effective partnership working
- Better knowledge of our customers resulting in improved service and user satisfaction.

Security of Information Assets

The Senior Information Risk Owner has the responsibility to provide an annual statement of the security of information assets, protecting the data that the organisation collects and stores securely. Key roles within the Council maintain the privacy of individuals and deliver Information Assurance (IA):

- Senior Information Risk Owner (SIRO) – Head of Corporate and Customer Services,
- Chief Information Owner (CIO) – Shared Service ICT Manager
- Data Protection Officer (DPO) – Corporate Information Manager
- Information Asset Owners (IAO) – List available from the Corporate Information Manager.

All colleagues understand that the information we hold is valuable. We are committed to preserving the confidentiality, integrity, and availability of our information assets:

- for sound decision-making;
- to deliver quality services to our citizens and customers;
- to comply with the law;
- to meet the expectations of our customers; and
- to protect our reputation as a professional and trustworthy organisation.

Roles and Responsibilities

Each Policy that sits beneath the overarching Information Governance Strategy contains detailed responsibilities for the Senior Information Risk Owner, Information Asset Owners and Data Protection Officer. A summary of those responsibilities are detailed below:

Senior Information Risk Owner (SIRO) and Information Asset Owners (IAOs)

The SIRO has overall responsibility for managing records and associated risks, whilst the IAOs have the responsibility to ensure information is held and used appropriately, retained for the correct period of time and then correctly disposed of or transferred to the archives.

In essence, the SIRO is supported by a team of specialists (IAOs), with day to day responsibility for records management. The IAOs are also responsible for ensuring their Teams comply with the retention schedule and ensuring it is reviewed and updated on a regular basis. They also have a role in supplying local expertise relating to retention periods and updating the relevant parts of the retention schedule in consultation with the Data Protection Officer.

Information Asset Owners
Information Asset Owners (IAOs) will also understand what information is held and who has access to it within their relevant Divisions, all of which will be retained in the Council's Information Asset Register.

Data Protection Officer
The responsibility for compliance with the GDPR is delegated to the Data Protection Officer (DPO). The DPO supports the implementation of this Strategy and associated Data Protection Policy and takes day to day responsibility for its operation. As part of the GDPR, the Council is required to appoint a DPO, who is responsible for the following activities:

- Keeping senior management informed on data protection matters
- Monitoring the Council's compliance
- Documenting, maintaining and developing policies and related procedures
- Educating employees on their responsibilities with regards to data protection and advising Officers on records management
- Providing advice on data protection impact assessments
- Embedding ongoing privacy measures into corporate policies and day-to-day activities
- Being the first point of contact for Subject Access Requests, deletion requests and queries from data subjects
- Checking and approving contracts (in conjunction with Procurement Lincolnshire) with third parties that process personal data to ensure they are compliant with GDPR before commencing the contract
- Working closely with ICT to ensure all systems, services and equipment used for storing personal data meet acceptable security standards
- Developing privacy notices to reflect lawful basis for fair processing, ensuring that intended uses are clearly articulated, and that data subjects understand how they can give and withdraw consent, or else otherwise exercise their rights in relation to the use of their personal data
- Co-operating wherever necessary with the relevant supervisory authority
- Providing advice and assistance regarding retention, disposal and transfer of information
- Ensuring that management of the Council's records complies with legal and professional obligations
- Maintaining the retention schedule.

Policy Review
This Strategy will be formally reviewed every two years to ensure it continues to be relevant and current. In some circumstances it may be necessary to review this Strategy more frequently in response to specific events.