South Kesteven District Council

Information Governance Guidance

May 2018

SOUTH KESTEVEN DISTRICT COUNCIL

Contents

1. Scope

1.1 This guidance applies to:

- All employees of the Council;
- Members of the Council;
- Suppliers and Contractors of the Council;
- Temporary and agency staff engaged by the Council;
- Volunteers at the Council;
- Others using the Council's information or systems.

1.2 The guidance covers all aspects of information within the Council, including (but not limited to):

- Personal and special category (sensitive) information (e.g. records about residents and staff);
- Other corporate information (e.g. financial or accounting records)

1.3 The guidance covers all information whether held in notes or structured records systems (paper and electronic) and the transmission of information (e.g. fax, e-mail, post and telephone etc.)

2. Purpose

2.1 'Information Governance' describes the framework by which organisations such as the Council handle information; it applies to special category (sensitive) and personal information of staff and also to information related to the business of the Council.

2.2 Effective Information Governance enables the Council to safeguard personal information and to make the best use of the information that it holds.

2.3 All staff have a responsibility at work to look after personal data properly and appropriately. Residents have a right to know that information about them is kept secure.

2.4 Breaches of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA), through loss or mishandling of personal data, can result in large fines for the Council and disciplinary action against individual members of staff which may lead to dismissal.

2.5 Information is also a valuable asset that helps to ensure that the Council provides the best possible services to residents.

2.6 Information plays a key part in effective governance, service planning, financial management and performance management. It is therefore important that information is well-managed and used effectively to deliver and improve services.

2.7 The Council will actively protect all paper and electronic data and information in ways that are appropriate and cost effective. The Council will thereby fulfil its statutory responsibilities, protect the interests of residents, partners, suppliers and businesses, and maintain the quality, effectiveness and continuity of services to South Kesteven residents.

2.8 This guidance provides an overview of the Council's approach to Information Governance; a guide to the policies and procedures in use; and the roles and responsibilities for managing information to ensure compliance with legal requirements.

3. Protocol

3.1 The Council will implement information governance effectively to ensure the following:

3.1.1 **Keeping information safe and secure**

- Information will be protected against unauthorised access
- Confidentiality of information will be assured
- Integrity of information will be maintained

3.1.2 **Recording accurately and only record what is required**

- Information will be supported by the highest quality data
- Only information that is required will be recorded

3.1.3 **Retaining and destroying records**

- Information will only be retained for as long as is required. Information will be destroyed securely as appropriate

3.1.4 **Accessible Information**

- Information will be accessible to those who have a right of access

3.2 The following ***information security principles*** guide this Protocol:

3.2.1 **Confidentiality** - Appropriate measures must be taken to ensure that information held by the Council is only accessible to those authorised to have access.

3.2.2 **Integrity** – The accuracy and completeness of information must be maintained and all changes or modifications affecting that information must be authorised, controlled and validated.

3.2.3 **Quality** - The Council must ensure that the information it holds is fit for its intended purpose.

3.2.4 **Availability** – Information must be available to authorised individuals when required. In the event of a disaster or malicious attack, the Council's information and systems critical to the operation of key services and ongoing activities must be recoverable.

3.2.5 **Authentication** – Any person or system seeking access to Council information or networks must first establish their identity to the satisfaction of the Council.

3.2.6 **Access control** – Access to view or modify information or systems must be restricted to those whose job functions specifically require such access.

3.2.7 **Auditing** – User access and activity on each of the Council's computers, firewalls and networks must be recorded and maintained in compliance with security, retention and all legislative and regulatory requirements.

3.3 The Council will monitor this guidance document, and will update it as necessary.

4. Legislation and Standards

4.1 The following legislation and standards are an integral part of the regulatory environment within which the Council must operate:

- The GDPR;
- Data Protection Act 2018;
- Freedom of Information Act 2000
- Human Rights Act 1998
- Environmental Information Regulations 2004
- Local Government Act 1972
- Computer Misuse Act 1990
- Payment Card Industry Data Security Standard

5. Roles and responsibilities

5.1 The following roles and responsibilities underpin effective Information Governance within the Council.

5.2 Senior Information Risk Owner (SIRO)

This role provides senior leadership for information governance in the organisation. The role:

- Ensures effective governance arrangements are in place for improving the management of information in the Council;
- Oversees the development of policies, procedures and guidance;
- Identifies organisation-wide information management risks and ensures appropriate action to mitigate risks are agreed and implemented;
- Ensures effective training and staff development is in place;
- Oversees any communications needed about information governance;
- Provides an annual report and updates as required to Corporate Management Team about the delivery and success of the information governance action plan.

5.3 Assistant Directors / Directors

5.3.1 Are accountable for the implementation of Information Governance, policies, procedures and guidelines in their service area.

5.3.2 Take ownership of the information in their service area.

5.3.3 Are accountable for identifying and managing effectively the information necessary for service delivery.

5.4 Business Managers

5.4.1 Ensure that staff in their team(s) are aware of policies, procedures and guidance for Information Governance.

5.4.2 Ensure that the practice of managing information in their service area complies with policies, procedures and guidance.

5.4.3 Must report breaches in data protection to the Council's Data Protection Officer.

5.4.4 Identify risks in managing information in their service area and ensure these are mitigated and/or escalated as required

5.4.5 Ensure that members of staff attend relevant and appropriate training.

5.5 Data Protection Officer

5.5.1 To inform and advise the Council and its staff who carry out processing of their obligations pursuant to the GDPR.

5.5.2 To monitor compliance with the GDPR and the DPA and with the Data Protection Policy and other Data Protection Policies and Procedures.

5.5.3 To act as the contact point for the Information Commissioner's Office on all matters relating to data protection and to fully cooperate with this body.

5.6 All Staff (whether permanent or temporary) and others using Council systems or information

5.6.1 Have a responsibility to ensure that they are familiar with the contents of this Policy and to ensure information is managed in line with Information Governance policies, procedures and guidelines;

5.6.2 Must report breaches of data protection to their Manager;

5.6.3 Are to undertake training and support as required.

6. Training and Guidance

6.1 All Information Governance related guidance and procedures are published on the Council's intranet and available to all staff. Staff are made aware of these procedures through well-established management and communication channels – such as check ins and PDRs, team meetings, training, staff communication channels and communications campaigns. All employees are required to complete the mandatory e-learning module on GDPR.

7. Incident Management:

7.1 Clear guidance on incident management procedures should be documented and staff should be made aware of their existence, where to find them and how to implement them.

7.2 See Procedure for Reporting Information Security Breaches, Data Protection Breaches and Card Data Security Incidents www.southkesteven.gov.uk/CHttpHandler.ashx?id=24185&p=0 for further information.