Derbyshire
DALES
District Council

Information Governance Framework 2018 – 2021

Approved 14 June 2018

Contents

1. Introduction

This framework sets out the approach taken by Derbyshire Dales District Council in the area of Information Governance. The Council recognises the importance of information to the daily work of the authority. Organisations gather information for the prime purpose of record keeping or making decisions. We do this by summating, aggregating and analysing data flowing through our operational systems. This is then used to form the basis of evidence-based decision making. By processing data and putting it into context we derive information, which we use to run our business. Intangible qualities such as knowledge and wisdom also help to shape information.

Information is gathered from a variety of sources, including customers, clients, stakeholders, government and partners. Information is a key resource, which if properly managed has a crucial role to play in enabling better decision making and delivering effective services to the community.

Types of information held may include financial data, property data, employee data, customer records, consultation data, equality data, polices, procedures, decision documents, transactional data, spatial data, publicity information etc. This information is captured in many different formats including letters, emails, reports, leaflets, web content, data sets, databases etc.

Councils must have in place an effective framework for collecting, accessing, storing, sharing and deleting information. It is even more important to have a consistent approach at times when the Council is continuing to experience budget pressures. Information technology has a huge role to play in providing and managing information.

This framework aims to outline our approach to Information Governance.

2. Principles

Information is a critical resource which must be effectively managed by the business in order for the Council to meet strategic aims, whilst meeting its obligation to the public. Taking into account our legislative, performance and policy responsibilities, the following key principles have been designed to set the direction of the Information Governance strategy:

- Information is actively and strategically managed as a critical business asset;
- Standard policies and procedures will be in place to implement legislative and regulatory requirements;
- We understand the information we have available and who is responsible for it;
- A strong focus on data quality is important to ensure information is accurate;
- Storage and security of information is managed effectively;
- Employees have the necessary skills to manage and use the information resources we hold;
- Availability and accessibility of information is managed efficiently to promote transparency;
- Sensitive or restricted or personal information is managed safely and information sharing is carried out with confidence;
- We will continuously strive to improve our Information Governance systems.

These principles will apply to all aspects of the council's work.

There are a number of national drivers which influence this strategy and the above principles. These include:

- Legislation and regulatory requirements (see below)
- Public Service Network (PSN) requirements
- Payment Cards Industry(PCI-DSS) requirements
- Contractual requirements such as the Public Sector Mapping Agreement and Data Co-operation Agreement.

The main legislation that guides this framework is:

- Data Protection Act 2018
- General Data Protection Regulation 2018 (GDPR)
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Regulation of Investigatory Powers Act 2000
- Re-use of Public Sector Information Regulations 2005
- Public Records Act 1958
- Local Government Act 2000
- Code of Recommended Practice for Local Authorities on Data Transparency (2011)
- E.U. INSPIRE Directive 2007/2/EC.

The ownership and governance of this framework will be through the following model:

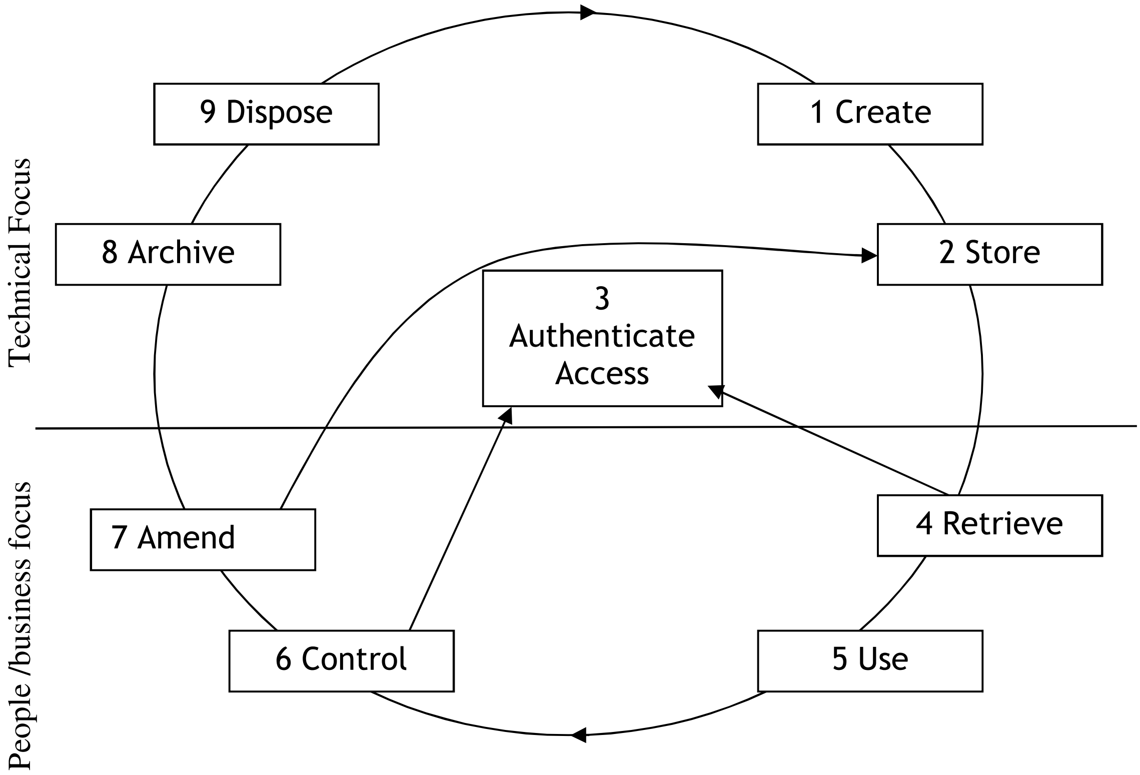
Governance Role	**Responsibility**	**Officer(s)**
Strategic Sponsor	High level sponsorship of the strategy and its implementation	Chief Executive
Information Governance Board	Sets the strategic direction for Information Governance and monitors progress	Head of Resources/Data Protection Officer Information Governance Officer Solicitor Business Support Manager Joint ICT Manager
Information Asset Owners	Ensuring the effective collection, storage, access, sharing and deletion of information within departments	Heads of Service / Senior Managers
Information Users	Safe and secure day to day authorised access and management of information	All employees, volunteers, agency staff and Members

3. Information Governance Requirements

Managing information involves a controlled and disciplined approach to looking after information assets at every step from creation through to disposal or indefinite retention to archive. High profile information losses from a range of both central and local government authorities and the introduction of financial penalties by the Information Commissioner's Office have only served to heighten the need for strong Information Governance in the public sector.

In order to understand our Information Governance requirements we must first identify how we obtain, use and dispose of information within the business. SOCITM have produced a model which sets out the different stages of the information life cycle which are helpful in clarifying Information Governance.

3.1 Information Life Cycle Model (SOCITM 2010)



The information life cycle model consists of:

1. Create	• Both systems and people create information. • Systems do so in an organised way whereas individuals are less so. • Making information available to those who have a legitimate right of access is imperative. • It is also important to avoid overloading people with information.
2. Store	• The important point of storing information is the ability to retrieve it easily later. • Information should be stored securely in line with policy.

	• Personal data should not be left on view in line with the Clear Desk Policy and Data Protection Policy
3. Authenticate Access	• The Information Security Policy should be followed at all times. • Security clearance needs to be in place for those that have a legitimate need to access information. • Setting up technical systems and rules about authentication is important. • Secure marking is also becoming an important element in line with the Information Security Policy.
4. Retrieve	• Retrieval is easier through electronic systems rather than manual files. • Research and retrieval tools should be utilised wherever possible.
5. Use	• Information will be used on a daily basis by employees and contractors to deliver services to customers. • Systems that process and present information need to support the user needs. • Information presented to customers must be easy to understand. • Information transfers within the organisation or with partners must occur in a secure manner in line with Information Sharing Protocols and the Data Protection Policy
6. Control	• Control is about establishing ownership, rights and responsibilities in relation to information. • Personal information (data) as defined by the Data Protection Act has to be strictly controlled. • Data sets should carry protective security markings. • Periodic and random audit checks on data quality and integrity should take place. • Data cleansing should be an ongoing activity.
7. Amend	• Amendments can be by employee interaction or automated. • Clear audit trails should exist when customer records are amended in line with the Data Protection Act. • Information contained in documents or data sets should have clear version controls.
8. Archive	• Archiving involves the removal of information to avoid clutter and preservation for future access. • The Document Retention Policy takes effect at this point in the life cycle. • Archived documents must be ordered, dated and readily retrievable.
9. Dispose	• At the final stage of the life cycle is the thorough destruction and disposal of information which must be done securely in line with guidelines. • Certificates of destruction should be maintained when data is destroyed by outside organisations.

For any model to be successful it needs to be backed-up with policies, procedures and employee learning/development.

3.2 Information Governance Policy and Procedures

There are a number of policies and procedures in place which help maintain the security of Council information assets. It is important that all employees are aware of their individual responsibilities to ensure that information relating to them, the Council and its customers, is protected.

The existing ICT policies are available on the intranet.

Freedom of Information and Data Protection policies, guidance and procedures can be found on the intranet.

Employees need to be aware of their own personal responsibilities, be prepared to report behaviour that is not in line with good Information Governance and understand the outcomes for breaching Information Governance controls.

3.3 Employee and Member Learning and Development

Information Governance skills should be considered as part of the recruitment and selection process for potential employees and as part of the induction process for employees and members. It is also important that competencies identify Information Governance as a core skill set to be discussed in the Staff Performance and Development Review process.

All employees and members will be required to undertake ICT Security Awareness training and mandatory Data Protection training. Training will be refreshed every two years.

4. Information Governance Structure

Information Governance is about ensuring that organisational information is managed as an asset to ensure that all statutory, regulatory, and best practice requirements are met.

Our approach is based on the following Information Governance Structure:

	Data Protection	Freedom of Information	Information Security	Records Management	Data Quality
Management Structure & Policies	For each framework heading there is a top level policy setting out the Council's rules, requirements and responsibilities. The Information Governance Board is responsible for implementing the framework				
Training & Awareness	There will be a planned approach to training and awareness for each policy. This will be regularly assessed, and should equip each person to fulfil their responsibilities				
Procedures & Documentation	There will be documented procedures to support agreed policies. These will specify any operational instructions required to ensure compliance with legislation and standards. All policies and procedures can be found on the intranet.				
New & Changed	Information governance issues will be considered for all new and changed information systems or deployment of ICT. The issues arising				

Systems	will be documented and assessed using information risk management methods where information assurance is identified as an issue. If the new or changed system processes personal data then a Data Protection Privacy Impact assessment will be required before implementation.
Monitoring & Compliance	There will be a timely and effective monitoring, reporting and compliance regime controlled through the Information Governance Board, including periodic reviews by Internal Audit.

The framework is designed to ensure that there is a structured approach to the improvement of information governance and to ensure that the District Council:

- Holds information securely and confidentially;
- Obtains information fairly and efficiently;
- Records information accurately and reliably;
- Uses information effectively and ethically;
- Shares information appropriately and lawfully.

The Council will monitor adherence to the framework through annual reviews of Personal Data Asset Registers. The framework itself will be reviewed every three years in line with Council Policy.