Information Governance Policy

Policy summary

Purpose	This policy defines a robust information governance framework that enables Dorset Council to meet the key requirements of legislation, including the General Data Protection Regulation (GDPR), government standards and established best practice, and essentially to manage, use and share data in an appropriate way. This policy outlines the strategic framework for managing information assets across the council, to obtain assurance that risks to information are effectively identified and managed. Information is a collective term used to refer to content, data, documents and records in all formats. Information is a valuable corporate asset that is indispensable to support business processes. This policy covers all personal and non-personal information that is created, received, managed, shared and disposed of by Dorset Council.
Scope	This policy applies to members, employees, casual and agency workers, volunteers, contractors and other third parties handling council information. It details the responsibilities of each of these roles, as well as specifically defining the named roles who are tasked with overseeing the assessment of information risk.

Table of contents

Information Governance policy summary 1
1. Introduction 4
2. Who this policy applies to 4
2.2 All employees, casual and agency workers, volunteers 4
2.3 Agency, contractors, third party suppliers 4
2.4 All managers 4
2.5 Members 4
2.7 Chief Executive 5
2.8 Senior Leadership Team 5
2.9 Audit and Governance Committee 5
2.10 Senior Information Risk Owner (SIRO) 5
2.11 Caldicott Guardians 6
2.12 Data Protection Officer (DPO) 6
2.13 Information Asset Owners (IAOs) 6
Policy details: 8
3. Information principles 8
4. Governance groups 8
5. Information Asset Register 9
6. Information risk management 10
7. Compliance 10
8. Organisational and technological change 10
9. Service design and delivery 10
10. Communications, learning and skills development 10
11. Monitoring compliance 10
12. Policy approval and review 10

Glossary

Information - data in context with a particular meaning. Information is a collective term used to refer to non-digital and digital, structured and unstructured data. Information is a vital, strategic asset.

Structured data - raw facts or figures that are usually stored in relational databases and organised in defined columns and rows.

Unstructured data - content held in documents, email, images, videos and web pages that are not organised in a pre-defined way.

Records - information created, received and maintained as evidence in the course of council business. Both unstructured and structured data can be managed as a record.

Archives - records selected for permanent preservation due to their evidential, cultural, or historical value.

Information governance - information governance is a strategic framework for managing information assets across the entire council to get the best value from information while minimising associated risks.

Senior Information Risk Owner (SIRO) - the role responsible for managing information risk at the highest level.

Information Asset Owner - designated senior managers responsible for monitoring the risks to information held in their service. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why.

Information champion - operational managers who are delegated tasks from an Information Asset Owner, to manage information on a day-to-day basis.

Information Asset Register - a simple catalogue to understand and manage information assets and the risks to them. The focus of the IAR is on the information content, whether stored on paper, digital or another format, not the systems that hold them.

Information Asset - any grouping of information, physical or digital, that has value in supporting your service's work.

1. Introduction

1.1 Information is one of the core assets of Dorset Council and is vital for the delivery of quality services and the efficient management of resources.

1.2 Information Governance consists of policies, procedures, roles and controls put in place to govern and control all information created, received, managed, shared and disposed of by the council.

1.3 This policy outlines the strategic framework of individual responsibilities, accountable roles, governance groups, and cooperation between information-related professionals, to build a culture that values information as an asset.

1.4 Information professionals advise on their areas of expertise in relation to corporate information risks and risks to individual information assets.

1.5 Information governance applies to all personal and non-personal information, regardless of its format, function or location. Managing information as an asset is not about IT systems but about taking ownership of the information content within and between systems to ensure it is of value, and not a liability, to the council.

2. Who this policy applies to

2.1 All employees, casual and agency workers, members, volunteers, contractors, partners, consultants and service providers are responsible for appropriately managing and storing the information they create and receive as part of council business.

2.2 **All employees, casual and agency workers, volunteers**

a) All users of council information are understanding and complying with this policy and associated policies.

b) Employees are bound by the code of conduct for employees to properly protect confidential data and not use it for unauthorised purposes.

c) Failure to comply with this policy or associated policies may result in disciplinary action.

2.3 **Agency, contractors, third party suppliers**

a) Complying with this policy and associated policies in line with their contract or agreement.

b) Failure to comply with this policy or associated policies may result in the termination of contracts or agreements.

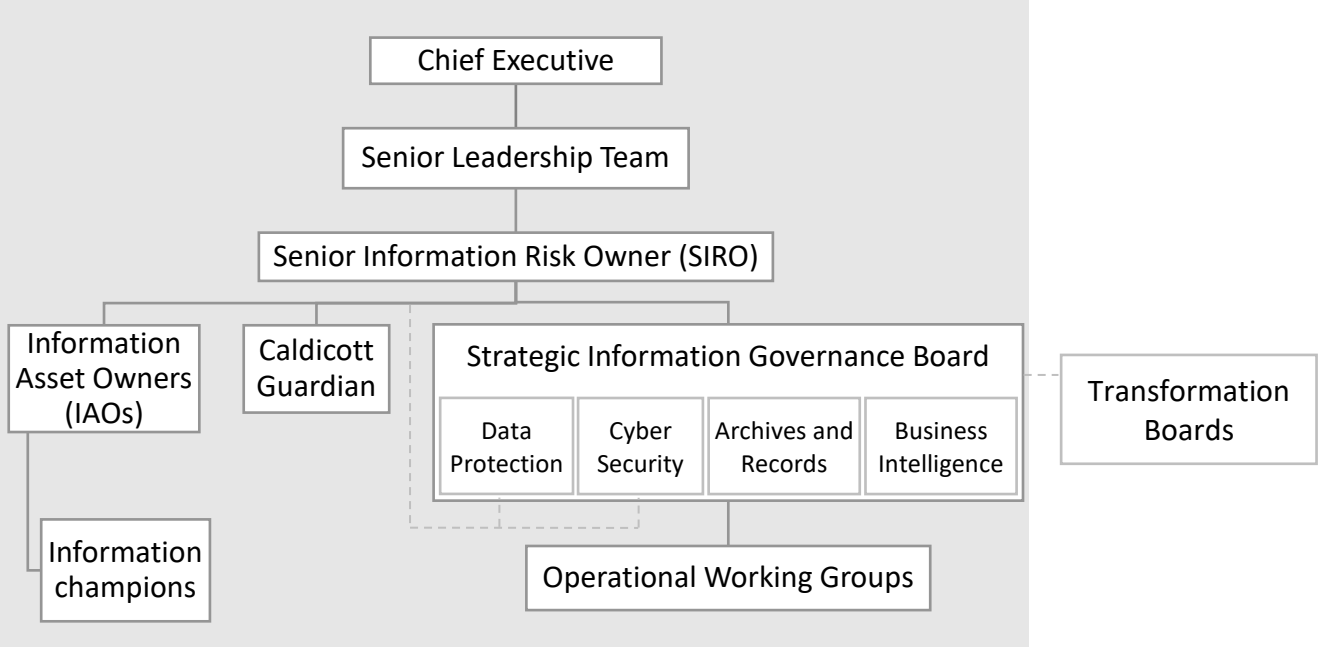
2.4 **All managers**

a) Implementing this policy and associated policies in their teams, including identifying and raising information risks with the relevant Information Asset Owner

2.5 **Members**

a) Complying with this policy and associated policies in line with the Members' Code of Conduct.

2.6 Certain roles within the information governance framework are specified, with duties as set out below.



2.7 **Chief Executive**

a) The Chief Executive has overall accountability for information governance.

2.8 **Senior Leadership Team**

a) The Senior Leadership Team (SLT) have oversight of information governance and are responsible for supporting initiatives within their directorates and service areas.

b) Executive Directors and directorate management teams have responsibility for the appointment of their directorate's Information Asset Owners and for collaborating on the definition and management of shared assets.

2.9 **Audit and Governance Committee**

a) Responsible for independent assurance on the adequacy of the Council's risk management framework including internal control and financial reporting.

2.10 **Senior Information Risk Owner (SIRO)**

a) The Senior Information Risk Owner (SIRO) is an SLT member responsible for managing information risk at the highest level.

b) Dorset Council's SIRO is the Corporate Director (Legal & Democratic Services).

c) The SIRO chairs the Strategic Information Governance Board and has overall responsibility for ensuring the Council's Information Asset Owners are carrying out their roles effectively.

d) Key responsibilities are to:

- Oversee the development of information governance policies and information risk management strategy

- Ensure that the council's approach to information risk is effective, in terms of resource, commitment and delivery
- Ensure that all staff are aware of the necessity for information governance and the risks affecting the council's information
- Provide a focal point for managing information risks and learning from incidents
- Prepare an annual information risk assessment for the Chief Executive to be included in the Annual Governance Statement

2.11 **Caldicott Guardians**

a) The Corporate Director for Adult Social Care Operations is the Council's registered Caldicott Guardian.

b) The Caldicott Guardian is a senior person responsible for protecting the confidentiality of service users' health and care data and making sure that it is used appropriately.

c) Key responsibilities are to:

- Act as the 'conscience' of the organisation and champion confidentiality issues with senior management
- Provide leadership and informed guidance on complex matters involving confidentiality and information sharing
- Ensure that the council satisfies the highest practical standards for handling personal information
- Register on the publicly available National Register of Caldicott Guardians

2.12 **Data Protection Officer (DPO)**

a) The DPO is an individual designated for the purposes of the GDPR, responsible for helping the council fulfil its data protection obligations.

b) Key responsibilities are to:

- Maintain expertise in data protection to provide advice on compliance with the GDPR and other data protection laws
- Monitor compliance with the GDPR and other data protection laws, and with the council's data protection polices
- Raise awareness of data protection issues, train staff and conduct internal audits
- Advise on and monitor data protection impact assessments
- Act as the first point of contact for the Information Commissioner's Office and for individuals whose personal data is held by the council

2.13 **Information Asset Owners (IAOs)**

a) IAOs are responsible for managing risks to the identified information assets in their service areas. Information assets are any grouping of information, in any format, that has value in supporting your service's work. For more information, see the **Information Asset Register** section below.

b) Dorset Council's IAOs are Service Managers or equivalent roles. Certain high-level assets are defined in the retention schedule and these are owned by Heads of Service or Corporate Directors.

c) Key IAO responsibilities are to:

- Lead and foster a culture that values, protects and uses information for the public good
- Know what information their assets hold, what enters and leaves them and why
- Know who has access to their assets and why, and ensure use of their assets are monitored
- Understand and address risks to the asset, and provide assurance to the SIRO
- Ensure the asset is fully used for the public good, including responding to information requests

d) IAOs must assess whether information assets are still required. If not, they are responsible for fully decommissioning them and disposing of information once it has passed its retention period defined in the Dorset Council retention schedule. Disposal of information is either by complete destruction or transfer to Dorset History Centre for permanent preservation.

e) IAOs must maintain entries for their information assets in the Information Asset Register and provide assurance to the SIRO about the management of their assets.

f) At least once a year, or sooner if there are changes, IAOs must formally review their information assets, assess the risks to their information and update the central Information Asset Register.

g) IAOs may delegate tasks to information champions but retain overall accountability for their information assets.

2.14 Information champions

a) Information champions are operational staff who are delegated tasks from the Information Asset Owner, to manage information on a day-to-day basis. Key responsibilities are to:

- Act as a local contact for information governance in the service area
- Ensure that information governance policies and procedures are followed
- Maintain accurate and up-to-date entries in the Information Asset Register
- Support the IAO in identifying and addressing risks to information

2.15 Information professionals

a) The Council recognises that some colleagues are information professionals who are experts in one or more information disciplines that make up information governance, including data protection, archives and records, cyber security and business intelligence.

b) These professionals sit on the Strategic Information Governance Board as advisors to provide support and guidance to the business decision makers. They will also support information governance at an operational level through the working groups that sit under the board.

Policy details:

3. Information principles

3.1 Our information principles[1] guide the future direction of work to support the information governance framework.

a) **Information is a valued asset** – information is an asset which is fundamental to the efficient and effective delivery of public services.

b) **Information is managed** – information is stored, managed, protected and exploited in a manner that reflects its value.

c) **Information is fit for purpose** – information must be accurate, valid, timely, relevant and complete to ensure that it meets the purposes for which it is intended.

d) **Information is standardised and linkable** – the opportunities for using information greatly increase when it is made available in standardised and linkable formats.

e) **Information is reused** – the value of information can be multiplied by re-use, and therefore opportunities to reuse should be looked for proactively.

f) **Information is published** – public information should be published, unless there are overriding reasons not to.

g) **Citizens and businesses can access information about themselves** – citizens and businesses should be able to access information about themselves, along with an explanation of how this information is used.

4. Governance groups

4.1 The Strategic Information Governance Board provides overall direction, influence, and leadership for information governance arrangements.

4.2 The Board is chaired by the SIRO, with the following decision-making members:

a) Caldicott Guardian (Vice Chair)

b) Chairs of the four operational working groups that sit below the board

c) Directorate Management Team representation from each Directorate

4.3 The Board is attended by professional and business leads who provide expert advice and support. These include professionals from Assurance, ICT Services, Legal Services, Digital and Change, Business Intelligence, HR and Archives and Records.

[1] These are a common set of principles used across the public sector. For more information see Information principles - The National Archives.

4.4 The strategic board is supported by four operational working groups, that escalate to the strategic board as required.

a) Information Governance Operational Group

b) Cyber Security Technical Group

c) Digital Applications Governance

d) Organisational Compliance and Risk Learning Group

4.5 Details of the responsibilities of each governance group will be defined in terms of reference and published on the intranet.

5. Information Asset Register

5.1 Dorset Council will maintain an up-to-date and complete Information Asset Register (IAR) to record data about all information of value held by the Council.

5.2 The IAR also acts as the Records of Processing Activities (ROPA) to meet Article 30 obligations of the UK General Data Protection Regulation (UK GDPR).

5.3 The IAR provides the basis for Information Asset Owners to assess how each asset is meeting its business need and for managing risks to this information.

5.4 Information assets are any grouping of information, physical or digital, that has value in supporting services' work. Information assets have value to the organisation, are not easily replaceable without cost, time, or skill, and impact services if they cannot be accessed.

"An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited efficiently. Information assets have recognisable and manageable value, risk, content and lifecycles." (The National Archives – Information Asset factsheet)

5.5 Information assets should be defined at a granular enough level that they group together the work that supports a particular business activity.

a) If information is used by more than one service, it should be described in one primary asset that has a single Information Asset Owner and referenced in other related assets.

b) Assets can contain other assets. For example, the retention schedule defines some information assets at a broad level, and these are either owned by Heads of Service or Corporate Directors. The Information Asset Register should precisely define information assets according to their service and its locality.

5.6 The IAR will be owned by the Data and Information Manager.

5.7 To ensure the Information Asset Register remains complete, the Data and Information Manager will undertake an annual audit. Information professionals will make regular spot checks.

6. Information risk management

6.1 Information risks will be handled in a similar manner to other major risks, such as financial, legal and reputational risks.

6.2 Risks to information will be identified, assessed and mitigated through the Information Asset Register process.

7. Compliance

7.1 The Council will ensure compliance with relevant legislation, codes of practice and government standards, including the NHS Data Security and Protection Toolkit online self-assessment tool.

8. Organisational and technological change

8.1 Information governance principles will be integrated into all relevant organisational processes e.g. change and project management, IT configuration and procurement.

8.2 Information governance responsibilities will be integrated into organisational structures and job roles.

9. Service design and delivery

9.1 The Council will use data and insights to drive improvement of our services. This is being delivered through a business intelligence & data strategy.

10. Communications, learning and skills development

10.1 All employees must complete mandatory information governance training, as part of their induction and on an annual basis, as described in the supporting policies.

10.2 Information professionals, IAOs and IAAs should receive specialist training relevant to their role. Additionally, leaders and board members including the SIRO and Caldicott Guardian should receive suitable training.

10.3 Awareness sessions will be provided to teams on request and regular reminders on information governance topics will be published through corporate communication channels.

11. Monitoring compliance

11.1 This policy will be supported by policies and strategies that will have their own monitoring and governance routes.

11.2 The Strategic Information Governance Board will monitor and report on overall progress of information governance.

11.3 The SIRO will produce an annual report on information governance activity for SLT and Audit and Governance Committee.

12. Policy approval and review

12.1 This policy will be reviewed every three years by the Strategic Information Governance Board or following any changes in legislation, regulations, or business practice.

Approved: Strategic Information Governance Board – 29 January 2024

Next review: January 2027

Policy Owner: Chair of Operational Information Governance Group (Service Manager for Assurance)