Ref. No.	CO/IG/3
Category:	
People	
Place	
Corporate	Yes
In Constitution	

Information Governance Policy

Policy Details

What is this policy for?	The Information Governance Policy describes the framework for how personal, confidential and corporate information is managed by Dorset Council.
Who does this policy affect?	All members, employees, students, apprentices, volunteers, contractors and other third parties handling council information.
Keywords	Information Governance, Information Asset Register, Information Asset Owners, Information Asset Administrators, SIRO, Caldicott Guardian
Author	Kate Watson, Information Governance Officer, Dorset Councils Partnership
Dorset Council policy adopted from	New policy for Dorset Council, which supersedes the below sovereign councils' policies: • Dorset County Council Information Governance Policy • Dorset Councils Parternship Information Governance Framework and Protocol
Does this policy relate to any laws?	Data Protection Act 2018; General Data Protection Regulation (GDPR); Freedom of Information Act 2000
Is this policy linked to any other Dorset Council policies?	This policy is part of the Information Governance Framework, which also includes: • Data Protection Policy • Data Breach Policy • Individual Rights Policy • Data Protection Impact Assessment (DPIA) Policy • Confidential Waste, Clear Desk and Screen Policy • Data Quality Policy • Protective Marking Policy • Records Management Policy • Records Retention Policy • Information Security Management Policy and related standards and protocols
Equality Impact Assessment (EqIA)	An EqIA screening tool was completed and submitted on 5th March 2019. The tool identified that there was no need to complete an EqIA.
Other Impact Assessments	N/A

Status and Approvals

Status	Live	Version	1.0
Last review date	This is a new policy	Next review date	1 April 2020
Approved by (Director)	Dorset Council Corporate Director: Legal & Democratic	Date approved	February 2019
Member/ Partnership Board Approval		Date approved	

Shadow Dorset Council

Information Governance Policy

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.*
Scope	*This overarching Information Governance Policy describes the framework for how personal, confidential and corporate information is managed by Dorset Council.* *Information is a collective term used to refer to content, data, documents and records in all formats. This policy covers all personal, confidential and corporate information that is created, received, managed, shared and disposed of by Dorset Council.* *This policy applies to all members, employees, students, apprentices, volunteers, contractors and other third parties handling council information.*

Table of contents

Shadow Dorset Council

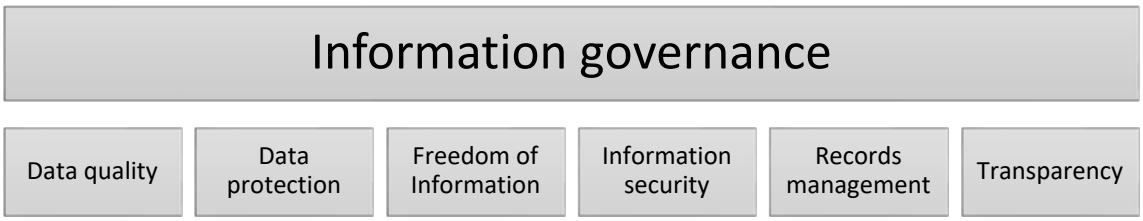
1. Introduction

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. Information Governance provides a coordinated approach for getting the best value from information while minimising associated risks.

1.2. Information Governance consists of a framework of overarching roles and responsibilities, policies, standards, procedures and guidance that covers all information disciplines and all information created, received, managed, shared and disposed of by Dorset Council.

1.3. This framework gives accountable roles to those working with information day-to-day in order to embed information governance as a core business function. Information professionals support all staff with expert advice.

1.4. Information governance applies to all personal, confidential and corporate information, regardless of its format, function or location. The information governance framework connects all information disciplines, as shown below:



1.5. Many different words or terms are used to describe concepts in information governance. The terms chosen for use in Dorset Council are explained in Annex A.

2. Information governance principles

2.1. Our information governance principles[1] describe expectations for information governance within Dorset Council and guide the future direction of the framework.

2.2. Dorset Council's information governance principles are set out below:

- Information is a valued asset
- Information is managed in a lawful way
- Information is fit for purpose
- Information is standardised, linkable and reusable
- Public information is published
- Residents and businesses can access information about themselves

2.3. The Council recognises that some colleagues are information professionals who are experts in one or more information disciplines that make up information governance. These professionals support information users to ensure that the principles are understood and applied consistently.

3. Information governance objectives

3.1. The overarching objectives for information governance are to:

- Maintain policies for each information discipline, with procedures and guidance where required

[1] Adapted from "Information principles for the UK public sector," 2011 [now withdrawn], accessed at https://www.gov.uk/government/publications/information-principles-for-the-uk-public-sector

- Maintain an up-to-date and complete Information Asset Register for all information assets held by Dorset Council
- Identify, assess and mitigate risks to information assets
- Integrate information governance principles into all relevant organisational processes e.g. change and project management
- Ensure compliance with relevant legislation, codes of practice and government standards, including the NHS Data Security and Protection Toolkit online self-assessment tool
- Ensure the quality of data so that it can be used to drive service design and delivery
- Inform staff, members, third parties and agents of the council regularly about information governance requirements and their responsibilities
- Provide sufficient resource to support the implementation of this framework

3.2. During the transition period, for the new Council, the focus of information governance will be to:

- Integrate information governance into organisational structures and job roles, process redesign activities and IT service configuration
- Embed information governance into the Dorset Council risk framework so that risks to information are considered in a similar manner to other major risks such as financial, legal and reputational risks
- Maintain compliance with the NHS Data Security and Protection Toolkit online self-assessment tool and other legislative, regulatory and industry standards
- Protect information and data during this period of change through the application of recognised procedures
- Provide easy to access advice and guidance to staff, members, third parties and agents of the council

4. Roles and responsibilities

4.1. Information governance is everyone's responsibility.

4.2. All information users with access to Council information are responsible for:

- Members
  - Complying with this policy and associated policies in line with the Members' Code of Conduct.
- Managers
  - Implementing this policy and associated policies in their teams, including identifying and raising information risks with the relevant Information Asset Owner.
- Employees (including temporary employees, contractors, consultants and volunteers)
  - Understanding and complying with this policy and associated policies.
  - Failure to comply with this policy or associated policies may result in disciplinary action in accordance with the Employee Code of Conduct, terms and conditions of employment and council disciplinary procedure.
- Agency, contractors, third party suppliers
  - Complying with this policy and associated policies in line with their contract or agreement.
  - Failure to comply with this policy or associated policies may result in the termination of contracts or agreements.

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

4.4. Chief Executive

- The Chief Executive has overall accountability for information governance.

4.5. Senior Leadership Team

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

4.6. Senior Information Risk Owner (SIRO)

- The SIRO is a Senior Leadership Team member responsible for managing information risk at the highest level. 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

4.7. Caldicott Guardian

- Caldicott Guardians are senior person(s) responsible for protecting the confidentiality of service users' health and care data and making sure that it is used appropriately. 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 publically available National Register of Caldicott Guardians

4.8. Data Protection Officer (DPO)

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

4.9. Information Asset Owners (IAOs)

- IAOs are senior managers responsible for information assets and assessing, controlling and mitigating risks to information in their service areas. Key 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 is 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

4.10. Information Asset Administrators (IAAs)

- IAAs are operational members of staff responsible for information assets 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

4.11. A list of all current appointees to specified roles will be maintained on the intranet.

5. Information Governance Board

5.1. The Information Governance Board provides overall direction and leadership for information governance arrangements. The Board is chaired by the SIRO, who is supported by professional and business leads. Key responsibilities are to:

- Lead and influence the direction of information governance
- Provide overall strategic direction and alignment of information governance with other organisational change work
- Work collaboratively to ensure successful information governance delivery
- Ensure that information governance is appropriately resourced
- Own the resolution of information governance issues, risks and decisions

6. Training

6.1. All staff must receive information governance training at induction and when receiving a new device. Further training may be provided to particular roles as appropriate.

6.2. Information governance 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.

6.3. Refresher training will be provided, as described in the supporting policies.

6.4. Awareness session will be provided to teams on request and regular reminders on information governance topics made available through corporate communication channels.

7. Related policies

7.1. During the transition period for the new authority, it is important that it is clear which policies and procedures are in force.

7.2. For a table of new information governance policies and which policies these have superseded, see the policy map in Annex B

8. Monitoring and review

8.1. Reporting on information risks is a core component of the overall framework. The Information Asset Register Procedure will describe the interfaces between the Information Asset Owners and the SIRO.

8.2. The Information Governance Board will monitor and report on overall progress of information governance, to include:

- Owning and monitoring corporate level information risks
- Commissioning audits of information governance practices
- Regular monitoring of KPIs
- Reporting on the information governance work programme
- Monitoring training activities completed by the organisation
- Producing SIRO reports, annual information governance reports and a statement for inclusion in the annual statutory governance statement

8.3. This policy will be reviewed annually by the Information Governance Board or following any changes in legislation, regulations or business practice.

Shadow Dorset Council

Annex A – Information governance definitions explained

Name	Information governance
Definition	Information governance is a framework for making information useful and reducing risk to the Council e.g. from non-compliance or reputational damage
What it is	Overarching roles and policies covering data quality, data protection, freedom of information, information security, records management and transparency
What it isn't	Locking information down so it's secure and compliant but nobody can use it

Name	Data quality
Definition	Recording and storing data so that it's fit for its original purpose and any secondary purposes
What it is	High quality data is accurate, timely, valid, relevant and reliable, complete and secure
What it isn't	Capturing every piece of data that could possibly be needed, data needs to be of the "right quality" for its purpose, not "top quality"

Name	Data protection
Definition	The fair and proper use of information that identifies, directly or indirectly, a living individual
What it is	Applying the UK data protection regime as set out in the Data Protection Act 2018 and GDPR to how the Council uses its local residents', service users', customers', and employees' personal information
What it isn't	It doesn't cover information about a person once they have died, but there is an ethical obligation that confidentiality still applies

Name	Freedom of information
Definition	The process of dealing with statutory requests for information under the Freedom of Information Act 2000 (FOIA) and the Environmental Information Regulations 2004 (EIR)
What it is	Requests for recorded non-personal information held by the Council
What it isn't	Releasing all Council information. Various FOIA exemptions and EIR exceptions may apply. However, the Council will proactively publish frequently requested information.

Name	Information Security
Definition	Information Security refers to the protection of physical or digital information, in any format, from unauthorized access, use, disclosure, modification or destruction
What it is	A combination of the right technical environment, policies, procedures and training. Security measures must maintain a level of security proportionate to the risk while still meeting user needs.
What it isn't	Reducing the risk to zero, the aim is to reduce the risk posed by technology choices, processes, human error and data storage

Name	Records management
Definition	The discipline responsible for the control of information selected to be kept for evidence or business reasons
What it is	Systematic maintenance of records from creation to destruction or transfer to the archives
What it isn't	Keeping things 'just in case'

Shadow Dorset Council

Name	Transparency
Definition	Transparency is about proactively opening up access to Council information. As a part of this, the Local Government Transparency Code sets out the minimum requirements for local authorities to publish open data for re-use.
What it is	Presenting information in useful, re-useable formats for public consumption
What it isn't	Only publishing the information specifically mandated by legislation. Dorset Council will proactively publish more information over time.

Shadow Dorset Council

Annex B – Policy map

Information discipline	Dorset Council Information Governance Framework		Superseded
	New Dorset Council policies, standards and procedures, and date applied	**Legacy policies, standards and procedures that apply during transition**	**Legacy policies superseded on 1st April 2019 unless specified otherwise**
Information Governance	• Information Governance Policy • Confidential Waste, Clear Desk & Screen Policy • Classification and Protective Marking Policy		• DCC Information Governance Policy • DCC Protective Marking Policy • DCP Information Governance Framework • DCP Information Governance Protocol
Data Protection	• Data Protection Policy • Data Breach Policy and Procedure • Individual Rights Policy • Subject Access Request Procedure • Data Protection Impact Assessment Policy and Procedure		• CED Personal Data and Security Incident Reporting • DCC Data Protection Policy • DCP Data Breach Policy • PDC Reporting Personal Data Breaches
Data quality	• Data Quality Policy		• PDC Data Quality Policy
Information Security	• Acceptable Use Policy • Information Security Management Policy and associated policies		• CED Acceptable Use Policy • DCC ICT Services Acceptable Use Policy • DCP Use of IT Protocol • PDC Computer Use Policy

Records Management	• Records Management Policy • Records Retention Policy and Common Activities Retention Schedule • Dorset History Centre Archiving Protocol	• DCC retention schedules except common activities • DCP Retention Schedule except common activities	• DCC Records Management Policy • DCC Common Activities Retention Schedule • PDC Records Management Manual
Freedom of Information	• Dorset Council will comply with the Freedom of Information Act 2000 and the Environmental Information Regulations 2004 in responding to information requests. • Dorset Council Access to Information document		• Joint Access to Information document
Transparency	• Dorset Council will comply with the Government's Transparency Code and will meet the statutory publication requirements		