



## Information Governance Framework

Document Control	
<b>Organisation:</b>	Gateshead Council
<b>Document Name:</b>	Information Governance Framework
<b>Purpose:</b>	To define the governance of information management within Gateshead Council
<b>Author:</b>	DPO Team
<b>Published version:</b>	
<b>Date published:</b>	
<b>Date of next review:</b>	2 years or sooner should changes to internal processes or legislation occur

Revision / Version History			
Date	Version	Author	Comments
28/06/2022	0.1 DRAFT	HH (DPO Team)	DRAFT document for discussion
20/09/2022	0.2 DRAFT	HH (DPO Team)	Draft for current IG structures with no reforms
29/09/2022	0.3 DRAFT	HH (DPO Team)	Clean copy with tracked changes removed
1/02/2023	0.4 DRAFT	HH (DPO Team)	Amendments made following consultation.
14/04/2023	0.5	ASM (DPO)	Final version to be submitted to Cabinet

Consultees to this policy	
<b>Title:</b>	DPO, SIRO, Service Director – IT, Cyber Security Group, Corporate Data Protection Group, SMG Service & Performance, CMT

Document Approvals	
This policy is required to be approved by:	Cabinet / Council

Distribution This policy and subsequent revisions will be distributed as follows:	
To	Method
All staff	Article included in weekly staff bulletin alerting staff of the publication of the updated policies and policies on the Council intranet.

## Table of Contents

Introduction.....	3
Purpose.....	3
Scope .....	4
Related documents.....	4
Information Governance Principles .....	4
Information governance structure.....	5
Responsibilities and roles.....	5
Members.....	5
Managers.....	5
Employees .....	5
Agency, contractors, third party suppliers.....	5
Chief Executive .....	6
Corporate Management Team.....	6
Senior Information Risk Owner (SIRO).....	6
Caldicott Guardian .....	6
Data Protection Officer (DPO) .....	6
Information Asset Owners (IAOs).....	7
Information Asset Assistants (IAAs) .....	7
Operational Groups .....	7
Training .....	7
Monitoring.....	8
Review.....	8

## Introduction

Information is one of the core assets of Gateshead Council (the Council) and is vital for the delivery of quality services and the efficient management of resources. It plays a key part in governance, service planning and delivery, and performance management.

The Council has a robust information governance framework to ensure that information, particularly personal, special category, sensitive and confidential information, is effectively managed with accountability structures, governance processes, documented policies and procedures, staff training and appropriate resources.

The framework gives accountable roles to those working with information day-to-day to reinforce information governance as a core business function.

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 the Council. 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:

Information governance					
Data quality	Data protection	Freedom of information	Information security	Records management	Transparency
<b>Policies</b> Why? identify issue, scope and responsibilities, for example, Data Protection Policy					
<b>Standards</b> What? Assign quantifiable measures, for example, encryption, passwords, acceptable use, data retention, roles and responsibilities, training					
<b>Procedures and Guidance:</b> How? Establish proper steps to take and accepted good practice, for example, Data Breach Procedure					

## Purpose

The information governance framework enables Gateshead Council to meet its information governance objectives and the requirements of legislation, including the UK General Data Protection Regulation (UK GDPR).

The Council's objectives for information governance are to:

- Maintain policies, procedures and guidance where required
- Maintain an up-to-date and complete Information Asset Register for all information assets held by the Council
- Identify, assess and mitigate risks to information assets
- Integrate information governance principles into all relevant organisational processes for example, change and project management

## APPENDIX 2

- Ensure compliance with relevant legislation, codes of practice and government standards
- Ensure the quality of data so that it can be used to drive service design and delivery
- Inform Members, employees, 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

### **Scope**

Information is a collective term used to refer to content, data, documents and records in all formats. This framework covers all personal, confidential and corporate information that is created, received, managed, shared and disposed of by the Council.

This framework applies to all Members, employees, students, apprentices, volunteers, contractors and other third parties handling council information. It is the responsibility of each Councillor, employee and employed contractor to adhere to this and any supporting policies, procedures and guidance. Third parties not directly employed by the Council but involved with Council information resources are expected to comply with the law and to accept and abide by the Council's information governance requirements.

### **Related documents**

The Information Governance Framework includes:

- Information Security Framework policies and related procedures
- Data Protection policies and related procedures
- Publication Scheme and Freedom of Information

### **Information Governance Principles**

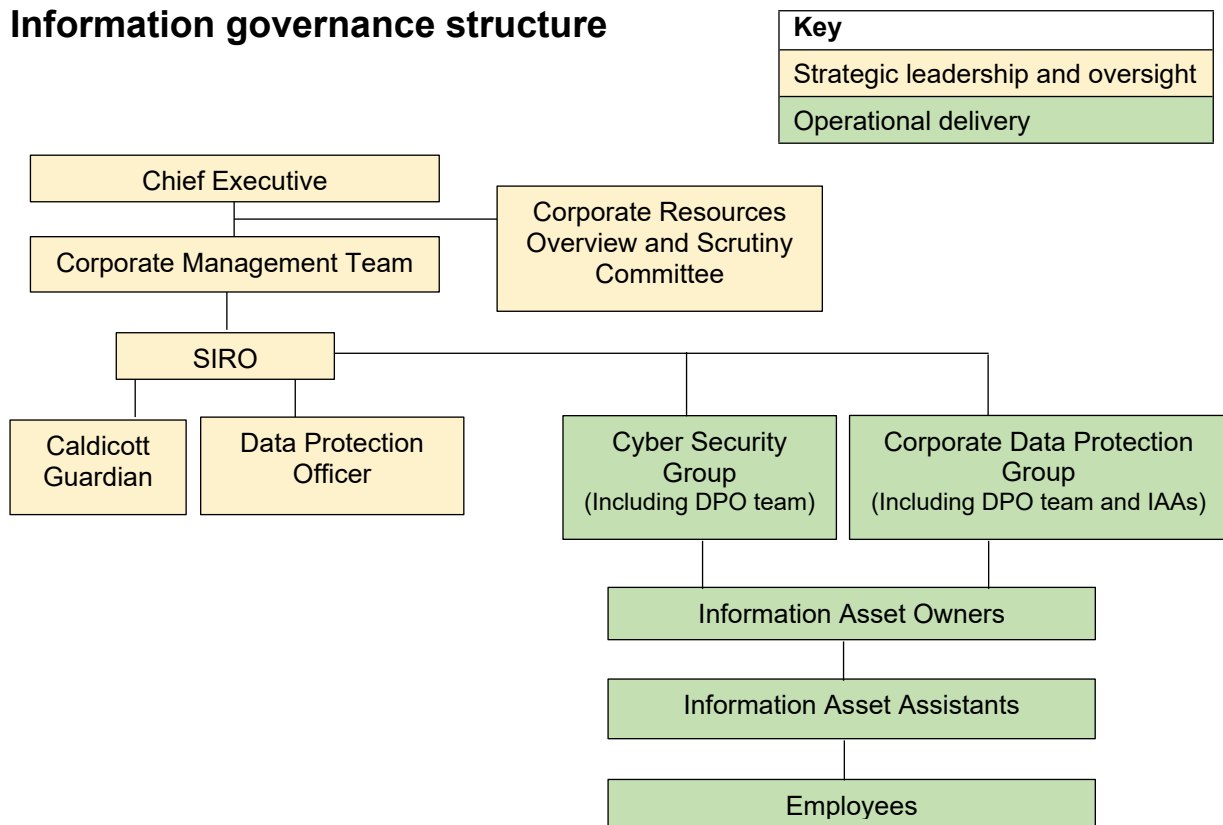
Our information governance principles describe expectations for information governance within the Council and guide the future direction of the framework.

The Council's information governance principles are set out below:

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

The Council recognises that some colleagues are information professionals in one or more information disciplines and who provide expert advice to information users.

## Information governance structure



## Responsibilities and roles

Information governance is everyone’s responsibility. Information users with access to Council information are responsible for:

### Members

- Complying with this policy and related policies in line with the Members’ Code of Conduct.

### Managers

- Implementing this policy and related policies in their teams, including identifying and raising information risks with the relevant Information Asset Owner (IAO).

### Employees (including temporary employees, contractors, consultants and volunteers)

- Understanding and complying with this policy and related policies.
- Failure to comply with this policy or related 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 related policies in line with their contract or agreement.
- Failure to comply with this policy or related policies may result in the termination of contracts or agreements.

Some roles have specific responsibilities:

### **Chief Executive**

The Chief Executive has overall accountability for information governance.

### **Corporate Management Team (CMT)**

The CMT has oversight of information governance across the council and are responsible for promoting and supporting good practice within their directorates.

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

The SIRO is a CMT member responsible for managing information risk at the highest level and who provides overall direction and leadership for information governance arrangements.

**The SIRO for Gateshead Council is the Strategic Director of Corporate Services and Governance.** Key responsibilities are:

- Overseeing the development of information governance policies and information risk management strategy
- Ensuring that the council's approach to information risk is effective, in terms of resource, commitment and delivery
- Owning the resolution of information governance issues, risks and decisions
- Providing overall strategic direction and alignment of information governance with other organisational change work
- Ensuring that all staff are aware of the necessity for information governance and the risks affecting the council's information
- Preparing an annual information risk assessment for the Chief Executive to inform the Annual Governance Statement
- Reporting to the relevant Oversight and Scrutiny Committee of the Council on the effectiveness of information governance controls

### **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 shared appropriately. The Guardian plays a key role in ensuring that the Council and partner organisations satisfy the highest practical standards for handling patient identifiable information. Their remit covers all social care records for children and adults. **The Caldicott Guardian for Gateshead Council is the Director of Integrated Adults and Social Care Services.** Key responsibilities are:

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

### **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. **The DPO sits within Legal & Democratic Services.** The DPO heads up the DPO team which provides operational and strategic advice and support to services in respect of data protection and wider information governance matters. Key responsibilities are:

- Maintaining expertise in data protection to provide advice on compliance with the GDPR and other data protection laws
- Monitoring compliance with the GDPR and other data protection laws, and with the council's data protection policies
- Raising awareness of data protection issues, training staff and conducting internal audits

## APPENDIX 2

- Advising on and monitoring data protection impact assessments
- Acting as the first point of contact for the Information Commissioner's Office and for individuals whose personal data is held by the council

### **Information Asset Owners (IAOs)**

**IAOs are senior managers (Service Directors)** responsible for information assets and assessing, controlling and mitigating risks to information in their service areas. Key responsibilities are:

- Leading and fostering a culture that values, protects and uses information for the public good
- Knowing what information their assets hold, and why
- Knowing who has access to their assets and why, and ensure use of their assets is monitored
- Understanding and addressing risks to the asset, and providing assurance to the SIRO
- Ensuring that information governance policies and procedures are implemented including responding to information requests
- Ensuring that records management and retention guidelines are implemented
- Ensuring information governance is appropriately resourced within their service

### **Information Asset Assistants (IAAs)**

**IAAs are operational members of staff nominated by IAOs.** Key responsibilities are:

- Acting as a local contact for information governance in their service area
- Representing their service area on the Corporate Data Protection Group and taking forward data protection work within their service area
- Maintaining accurate and up-to-date entries in the Information Asset Register
- Supporting the IAO in identifying and addressing risks to information

A list of IAAs will be maintained on the intranet.

### **Operational Groups**

Operational groups (the Corporate Data Protection Group and the Cyber Security Group) deliver the information governance work programme. Each group reports to the SIRO with responsibilities that include:

- Working with services to embed the information governance principles
- Providing a focal point for managing information risks and learning from incidents
- Developing and reviewing policies, procedures and guidance for their information disciplines
- Reviewing and reporting on data protection compliance in their information area

## **Training**

All staff will receive information governance training at induction. Further training may be provided to particular roles as appropriate.

Information governance professionals, IAOs and IAAs will receive specialist training relevant to their role. Additionally, leaders including the SIRO and Caldicott Guardian will receive suitable training.

Refresher training will be provided as described in the related policies.

## **Monitoring**

Reporting on information risks is a core component of the overall framework

The SIRO 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
- Reporting on the information governance work programme
- Monitoring training activities completed by the organisation

## **Review**

This framework will be reviewed as it is deemed appropriate, but no less frequently than every 2 years.