Information Governance Management Framework

Document Control

Organisation	Gravesham Borough Council
Title	Information Governance Management Framework
Author	Tejinderpreet Lalli, Head of Information Governance (DPO)
Filename	Gravesham Borough Council Information Governance Management Framework
Owner	Information Governance & Strategy Group (IGSG)
Subject	Information Governance
Protective Marking	Public
Review date	August 2024

Revision History

Revision Date	Revisor	Previous Version	Reason for revision
16/09/2020	Gayle Jones	n/a	Development of IGM Framework
01/02/2024	Sarah Parfitt/David Herrington/Tejinderpreet Lalli	1.0	Revision due
01/08/2025	Digital Team		Reformatted for accessibility

Document Approvals

This document requires the following approvals:

Sponsor Approval	Name	Date
IG Strategy Group Chair	Sarah Parfitt, Director, Corporate Services	
Management Team	Stuart Bobby, Chief Executive	

Document Distribution

This document will be distributed to:

Name	Distribution method
All council employees who handle personal data and Elected Members	Via staff Intranet and email
All employees of shared services commissioned by the council who handle personal data of which GBC is the data controller.	Via agreed process.
Publication	Council Website

Gravesham Borough Council

Contents

Introduction

Information is a vital asset for the provision of services to the public and for the efficient management of council services and resources. As well as rights to access public and personal information, it plays a key part in governance, service planning and performance management. Gravesham Borough Council's Code of Corporate Governance states:

"Governance is about how authorities ensure they are providing the right services to the right people in a timely, open, honest and accountable manner."1

Information governance is concerned with how information is held, obtained, recorded, used and shared by the organisation.

Information is used here as a collective term to cover terms such as data, documents, records and content.

It is essential that the council has a robust information governance management framework, to ensure that information is effectively managed with accountability structures, governance processes, documented policies and procedures, staff training and adequate resources.

Senior roles

Cabinet and Portfolio Holder

Full Council remains the ultimate policy-making body of the Council. In particular, it proposes the policy framework and budget to the Council and then carries on the work of the Council within this approved framework and budget.

The Cabinet Member for Performance & Administration has specific service responsibility for Information Governance. The Leader of the Executive has specific service responsibility for IT Services and is the council's Cyber Champion.

Chief Executive and Corporate Board

The Chief Executive is the Head of Paid Service who leads the council's staff and advises on policies, staffing, service delivery and the effective use of resources. Together with the Directors and the Deputy Monitoring Officer they form the council's Management Team ensuring delivery of an effective council-wide information management approach.

Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner (SIRO) has overall responsible for managing information risk in the council and chairs the Information Governance Strategy Group. The SIRO is the Director (Corporate Services) who has responsibility to:

- foster a culture for protecting and using information within the council
- ensure arrangements are in place to deliver information governance compliance with legislation and council policies
- provide a focal point for managing information risks and incidents
- prepare an annual information risk assessment for the council.

The Assistant Director (Organisational Development & Democratic Support) is designated as the Deputy Senior Information Risk Officer.

Key policies

The key policies in the framework are:

- Data Protection Policy

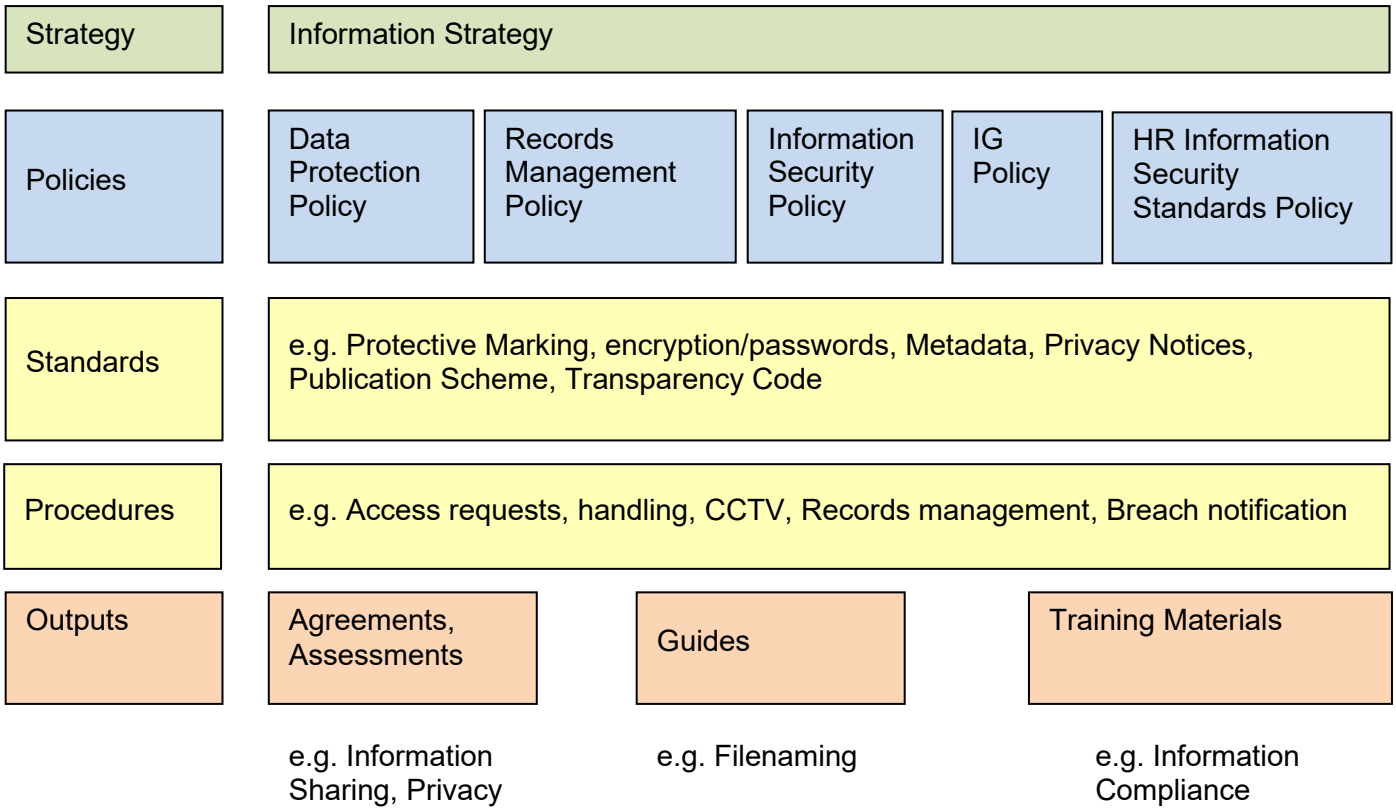
---

[1] Code of Corporate Governance for Gravesham Borough Council

- Records Management Policy
- Data Breach Policy
- Anonymisation & Pseudonymisation Policy
- Subject Access Request Policy
- Information Security Policy Overview
- Information Sharing Policy
- HR Information Security Standards Policy

These policies are supported by standards and procedures shown in the framework diagram. Outputs will be produced from use of these standards and templates, for example data protection impact assessments, awareness guides and training material.

Information Governance Framework



Key Governance Bodies

The Information Governance Strategy Group's responsibility and purpose are to:

1. Approve and ensure that a comprehensive information governance framework, supported by policies, standards, procedures and systems are in place and operating effectively.
2. Prepare any annual Information Governance / Risk Assessment required, including action plans.
3. Coordinate Information Governance activities (GDPR, DP, FOI/EIR, security, quality, records management) across the council.
4. Monitor information handling and breaches, implement assurance controls (including audits as required) and determine and monitor the implementation of corrective actions where needed.
5. Ensure training and action plans for information governance are progressed throughout the council, evaluating the impact and effectiveness of governance training.
6. Communicate the information governance agenda and the work of the IG Strategy Group to MT, GBC staff and Members where necessary.

Resources

The Information Governance Team provide expert advice and guidance to all staff on all elements of Information Governance. The team is responsible for:

1. Providing advice and guidance on Information Governance to all staff.
2. Developing the Information Strategy, Information Governance Framework of policies, standards and procedures.
3. Working with information governance coordinators and service teams to establish protocols on how information is to be used and shared.
4. Developing Information Governance awareness and training modules for staff.
5. Ensuring arrangements are in place to deliver compliance with Data Protection, Freedom of information, Records Management, Information Security and other information related legislation.
6. Recording and monitoring of information requests and supporting request handlers and service teams with processing requests.
7. Integrating Government and Information Commissioner specific Information Governance guidance, policies and codes of practice into council policies and procedures.
8. Providing support to the Senior Information Risk Owner for Information Governance related issues.

IT Services are the lead for technical security management of the infrastructure and technical security advice, including areas such as PSN Code of Connection, PCI-DSS and device policy.

The Legal Services team provide expert legal opinion on all information governance matters to all service teams, including the Information Governance and IT teams.

There will be identified roles such as Information Asset Owner in the service areas whose remit includes some aspects of information governance and ensuring compliance. These will vary according to the services provided.

Governance framework

Directorate Management Teams are accountable for the effective management of information risk and information governance compliance, as well as supporting and

promoting the policies, standards and procedures. The teams comprise of the Director/Assistant Director and Heads of Service for each business unit.

Each **Assistant Director/Head of Service is an Information Asset Owner** who is accountable for information assets within their business unit. They are able to understand how it is held, used and shared and address risks to the information.

All council **managers** are responsible for the implementation and adherence of this framework and any associated standards and procedures within their service and teams. Compliance with this is verified each year through Assurance Statements completed by all Directors/Assistant Directors and Heads of Service as part of the council's annual Governance Review.

Disregard for information governance policies by employees may be regarded as misconduct to which the council's Disciplinary Procedure applies and a serious breach of any policy may be treated as gross misconduct and may lead to dismissal.

Disregard by contractors and agents working for the council will be regarded as a contractual breach. Disregard by volunteers and work experience students working for the council may lead to terminating their work agreement.

Training and guidance

Information Governance training for all staff will be mandatory as part of induction, to include all employees, secondees, agency and voluntary staff. This will be through e-learning modules that are accessible on any device.

Further modules as appropriate to the role will be available through e-learning or classroom session, developed internally or through recognised providers.

Awareness sessions may be given to staff as required, at team meetings or other events.

Regular reminders on information governance topics are made through corporate and local team briefings, staff news and emails.

Policies, procedures, standards and advice are available to staff at any time on the staff intranet

Incident management

The Data Breach Policy details data incident reporting procedure and is available to all staff, with a reporting form available for download.

Staff aware of a potential or actual incident are required to complete the form as fully as possible and send this to the Data Protection Officer/ Information Governance Team at gdpr@medway.gov.uk as soon as possible and **within 24 hours.** Immediate actions should be taken to recover or reduce the risk of loss.

Incidents are reported to the Information Governance Strategy Group to monitor and agree any corporate actions required.

Monitoring and review

This framework and the supporting standards will be monitored and reviewed bi-annually in line with legislation and codes of best practice.

Further Information

Information Governance Team, Gun Wharf, Chatham, Kent, ME4 4TR

Email: gdpr@medway.gov.uk

External legislation

General Data Protection Regulation

Data Protection Act 2018

Human Rights Act 1998

Freedom of Information Act 2000

Environmental Information Regulations 2004

Privacy and Electronic Communications Regulations

Local Government Acts

Computer Misuse Act 1990

Common Law

Duty of Confidentiality

This is not a written Act of Parliament. It is “common” law. This means that it has been established over a period of time through the Courts.

It recognises that some information has a quality of confidence, which means that the individual or organisation that provided the information has an expectation that it will not be shared with or disclosed to others.

For information to have a quality of confidence it is generally accepted that it:

- is not “trivial” in its nature
- is not in the public domain or easily available from another source
- has a degree of sensitivity
- has been communicated for a limited purpose and in circumstances where the individual or organisation is likely to assume an obligation of confidence. For example information shared between a social worker/client, health practitioner/patient, etc.

However, as with the Human Rights Act, confidentiality is a qualified right. The Council is able to override a duty of confidence when it is required by law, or if it is in the public interest to do so.