Information Governance Framework

Author: Rachel Everitt

Date: September 2024

Version: v2.0

Title	**Information Governance Framework**
Author	**Rachel Everitt**
Owner	**Data Protection Officer**
Created	**4 June 2021**
Approved by	**Audit Committee**
Date of Approval	
Review Date	**October 2026**

Document Version Control

Document Version Control	
Issue Number	Date
1.0	04 June 2021, Audit Committee
2.0	October 2024

This is a live document effective from the issue date. It supersedes any previous versions of this document, which are now withdrawn.

Contents

1. Introduction

Information is a key corporate asset that requires the same discipline to its management as is applied to other important corporate assets such as finance, people and facilities, to enable better decision making and delivering effective services to our communities, residents, service users and staff.

Council access, store and create a wide range of information and data in many different formats through its day-to-day operations.

It is therefore imperative to have an effective framework for collecting, accessing, storing, sharing and deleting information across all services, that is sufficiently robust, consistently applied and statutorily compliant is in place.

This Information Governance (IG) Framework outlines our approach to the effective management of information and data through the identification of key roles and responsibilities and development of policies and procedures, along with best practice and standards for managing the information assets.

This IG Framework, which has been developed to take account of the standards set by the Information Commissioners Office and other relevant legislation and guidance, is an essential element of the wider corporate governance agenda and interlinks with other governance arrangements such as audit, risk, business continuity and information technology / digital management.

Scope

This framework applies to all Council employees and all organisations acting on behalf of the Council.

Through the implementation of the Information Governance Framework the Council aims to:

- strategically and actively manage information as a critical business asset;
- understand the information available, needed and retained, including

sensitive, restricted, personal or special class information;

- ensure that all information is complete, accurate, accessible and useable by those with a legitimate need and legal basis;
- establish, implement and maintain local policies, procedures and guidelines that comply with legislative and regulatory requirements to enable the effective management of data processed;
- effectively manage the storage and security of information;
- ensure information is publicly accessible and provide clear guidance about how information is recorded, handled, stored, shared and managed to promote transparency;
- provide clear advice, guidance and training to all staff, irrespective of contractual status, to ensure that they understand and apply the principles of robust information governance to their working practice;
- develop and sustain an Information Governance culture through increasing awareness and promoting good information governance practice thus minimising the risk of breaches;
- assess corporate performance using the Data Security and Protection Toolkit and Internal Audits, developing and implementing action plans to ensure continued improvement as required.

Legislation

This framework is based on the following legislation:

- Data Protection Act 2018
- Health and Social Care Act 2012
- Freedom of Information Act 2000
- General Data Protection Regulation 2018
- A guide for confidentiality in Health and Social Care
- Common Law Duty of Confidentiality
- Caldicott Guidance
- Access to Health Records Act 1990
- Public Records Act 1958
- Environmental Information Regulations 2004
- Regulation of Investigatory Powers Act 2000
- Re-use of Public Sector Information Regulations 2005

- Local Government Act 2000
- Code of Recommended Practice for Local Authorities on Data Transparency (2011)
- Computer Misuse Act 1990
- Human Rights Act 1998
- Information Security Standard ISO 27002:2005
- Records Management Code of Practice for Health and Social Care 2016
- Mental Capacity Act 2005
- ICO guidance and goo practice
- Notification of data Security and Protection Incidents (May 2018)
- Openness of Local Government Bodies Regulations 2014

This is not an exhaustive list and will be reviewed on a regular basis.

2. Roles and Responsibilities

Information Governance is the responsibility of all employees and contractors working on behalf of the Council and wilful or negligent disregard for information governance policies and procedures will be investigated and may be treated as a disciplinary matter which could lead to dismissal or the termination of work agreement or service contracts.

The following specific roles and responsibilities are applicable in respect to this Framework:

Chief Executive

The Chief Executive for Bury Council has overall responsibility for Information Governance which includes the effective management through appropriate mechanisms which support service delivery and continuity.

Senior Information Risk Officer (SIRO)

The SIRO (Director of Law and Governance) has responsibility for information as a strategic asset of the organisation and ensuring that the value of this asset to the organisation is understood and recognised and that measures are in place to protect against risk.

The SIRO has a key role in ensuring that the organisation:

- identifies and manages its information risks;
- implements robust information asset management arrangements;
- reviews and agree actions in respect of identified information risks; and
- ensures sufficient resources are in place to manage the information governance agenda.

Data Protection Officer (DPO)

The GDPR introduces a legal duty for all public authorities and organisations that carry out certain types of processing activities to appoint a Data Protection Officer (DPO).

DPOs assist to monitor internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments, (DPIAs) and act as a contact point for data subjects and the supervisory authority (ICO).

The DPO must be independent, an expert in data protection, adequately resourced, and report to the highest management level.

Caldicott Guardian

The Caldicott Guardian(s) are responsible for protecting the confidentiality of people's health and care information and for making sure it is used properly. They will act as an advocate for information sharing at a strategic level and in internal discussions. Key tasks will include:

- Ensuring that the organisation and its partner organisations satisfy the highest practical standards for handling patient and service user information;
- Acting as the 'conscience' of the organisation in relation to information sharing and supporting work to enable information sharing where it is appropriate to do so; and
- Advising on options for lawful and ethical processing of information.

There will be an identified Caldicott Guardian for Adult, Children and the health and care commissioning.

Policy and Compliance Team

Working under the direction of the DPO, the Policy and Compliance Team are responsible for ensuring the day-to-day delivery of the Information Governance agenda, including oversight and delivery for all aspects of data security and data protection.

The Policy and Compliance will ensure that in addition to internal relationships with identified IG post holders, they will also foster good relationships across Greater Manchester in respect and specifically with GMCA Senior IG Lead and ensure any regional guidance is reflected into local practice as necessary.

Heads of Service (Information Asset Owners)

The Information Asset Owners (IAO) are senior members of staff who understand the overall business goals of the organisation and how the information assets they own contribute to and affect these goals. An Information Asset is any form of information that has a value to the organisation (for example personal development plans, or complaint records) and is recorded on a departmental Information Asset Register (IAR).

All Managers (Information Asset Managers)

The Information Asset Managers (IAM) have day to day management responsibility of the information assets used in their business area. They usually use them more frequently than an IAO and can identify the risks associated with the assets they use and how to ensure continued compliance with legislation.

All staff (Information Asset Administrators)

All employees and individuals working on behalf of the Council are Information Asset Administrators (IAA) and have a responsibility to be the 'eyes and ears' that help keep the organisation safe and compliant, report when things may have gone wrong, keep asset registers up-to-date and highlight information risk,

issues and concerns as they emerge. The IAAs are collectively responsible to achieving Information Governance success.

3. Information Governance Framework

The Information Governance Framework sets out the way Bury Council handles information, in particular, the personal and sensitive data of our customers and employees.

The framework includes the following policies, procedures and guidance:

1. Appropriate Policy – Processing Special Categories of Data
2. Data Protection Impact Assessment Guidance
3. Data Protection Policy
4. Data Quality Policy
5. Data Sharing Guidance
6. Data Subject Rights Policy
7. Disposal of confidential waste guidance
8. Freedom of Information and Environment Information Regulations Policy
9. Freedom of Information Publication Scheme Policy
10. Information Governance and Data Protection Complaints Policy and Procedure
11. Information Governance Incident (Data Breach) Procedure
12. Information Records Management guidance
13. Information Retention Policy
14. Information Security Policy
15. Information Technology Security Policy
16. Privacy Notices (available here)
17. Pseudonymisation and Anonymisation Policy
18. Redaction guidance
19. Subject Access Request Policy

4. Governance and Reporting Arrangements

Audit Committee

The Audit Committee is responsible for proving assurance on the Council's audit, governance (including risk management and information governance) and financial processes in accordance with the functions scheme.

Corporate Governance Group (CGG)

This group brings together strategic leads who support the Information Governance agenda, including the SIRO, Data Protection Officer, and representatives from each department, and has a remit to:

- Approve and ensure a comprehensive information governance framework, policies, standards, procedures and systems are in place and operating effectively;
- Oversight and approval of all annual Information Governance / Risk Assessment required, including action plans and the annual submission of compliance with the requirements in the Data Security and Protection Toolkit;
- oversee the development of information sharing agreements;
- promote the Information Sharing Gateway for recording and monitoring information sharing across partnerships;
- act as an advisory group on implications /developments of information governance when setting up systems and projects;
- Oversight and coordination of Information Governance activities (data protection, information requests, information security, quality, and records management);
- Monitor information handling and breaches, implement assurance controls (including Data Protection compliance audits as required), take corrective actions and share the learning from these;
- Ensure training and action plans for information governance are progressed and evaluate the impact and effectiveness of governance training; and
- Oversee the communication plan that supports the information governance agenda

Strategic Leadership Group (SLG) and Senior Managers Forum (SMF)

SLG and SMF will bring together the Information Asset Managers to ensure all operational aspects of information governance are progressed and compliance with required internal and external assessments (e.g. internal audits, DPST) including:

- Identify gaps in processes/ procedures that may have implications for Information Governance;
- Establishment of Information Asset Registers and Data Flow mapping across all teams;
- Keep under review Information Asset Registers by department;
- Keep under review Data Flow Mapping registers by department;
- Keep under review Record of Processing Activities (ROPA);
- Keep under review and co-ordinate DPIA and DSA registers;
- Oversee delivery of actions arising from data breaches;
- Provide updated on departmental performance in respect to SARs and FOIs; and
- Contribute to and prepare compliance reports with annual assessments and audits.

5. Training

This framework is communicated to all staff through regular corporate communications including team briefings, staff newsletters and e-mail communications. All staff are expected to understand the framework and how it applies to their role.

As a minimum all staff are required to complete the mandatory IG training module on an annual basis. Failure to complete the module may result in access to IT services being removed.

All new starters must complete the IG training module within one week of their initial day working for the Council.

The SIRO, DPO, Caldicott Guardian(s) and Policy Compliance Team will receive additional in-depth training consummate to their role. Other staff may be required to attend additional training on specific areas of Information Governance dependent on their role.

6. Compliance and Monitoring

The Information Governance Framework will be monitored and reviewed annually in line with legislation and codes of practice

Bury Council will continue to review the effectiveness of this framework to ensure that it is achieving it intended purpose.

Any breaches of the principles in this policy must be reported to the information governance team immediately; ig@bury.gov.uk.

Where staff fail to follow and comply with this policy it may result in disciplinary action via the HR channels.