# INFORMATION GOVERNANCE FRAMEWORK

2022-23

## Further information regarding this document

| | | |
|---|---|---|
| **Document name** | Information Governance Framework | |
| **Author(s)**<br>**Contact(s) for further information about this document** | Interim Information Governance and Risk Strategic Advisor - NHS Bury CCG and Bury Council<br>Corporate Core - Governance and Assurance | |
| **This document should be read in conjunction with** | | |
| **Supersedes** | Data Security and Protection Framework v7.0 (CCG) | |
| **This document has been developed in consultation with** | Data Protection Officer, Bury Council<br>Director of Corporate Core Services, Bury Council | |
| **This document has been ratified by** | 21 June 2022 | |
| **This document will be reviewed in** | 12 months | |
| **Published by** | **NHS Bury CCG**<br>Townside Primary Care Centre<br>1 Knowsley Place, Knowsley Street, Bury, BL9 0SN<br>**www.buryccg.nhs.uk** | **Bury Council** |

### Version Control

| Version | Date | Reviewed by | Comment |
|---|---|---|---|
| v0.1 | 30/12/2020 | Deputy Director Governance and Assurance | Initial draft submitted for wider review |
| v0.2 | 11/01/2021 | Deputy Director Governance and Assurance | Table at 3.2 updated |
| v0.3 | April 2021 | Reviewed by JET | Supported |
| v1.0 | 28/05/2021 | Information Governance Steering Group | Approved and Ratified |
| V1.1 | 25/05/2022 | Interim Information Governance and Risk Strategic Advisor | |
| V2.0 | 21/06/2022 | Bury Council Information Governance Steering Group | Approved |

# Contents

## 1.0 Introduction

1.1 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, patients and staff.

1.2 In the course of day-to-day operations, the CCG and Council access, store and create a wide range of information and data in many different formats.

1.3 It is therefore imperative to ensure 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.

1.4 This Information Governance 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.

1.5 This Information Governance Framework, which has been developed to take account of the standards set by the Information Commissioners Office (ICO) 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.

1.6 All references to the General Data Protection Regulation (GDPR), imply the UK GDPR, which came into effect in January 2020 as a result of the UK leaving the European Union.

## 2.0 Purpose and Scope

2.1 Good information management is vital to ensure the effective and efficient operation of services, the meeting of standards and compliance with legislation and for demonstrating accountability for decisions and activities.

2.2 This framework therefore applies to all CCG and Council employees and all individuals or organisations acting on behalf of the CCG and / or Council.

2.3 The framework is not directly applicable to schools or GP practices who remain data controllers in their own right, however it can be called upon as needed, along with other underpinning Information Governance policies to support and enable the discharge of duties.

2.4 Through the implementation of the Information Governance Framework the CCG and 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.

2.5 The benefits of the framework will be:

- increased efficiency through the more effective use of physical, electronic and human resources;
- better service delivery through improved access to relevant information making requests easier to handle in a shorter time and in line with statutory timeframes where applicable;
- contribution to improved environmental benefits by reducing reliance on paper files and physical storage;
- more agile working through the removal of irrelevant information and documentation from static office bases with a shift to cloud-based retention of essential documentation allowing staff easier access to the information required to perform their work; and
- improved compliance with legal requirements through promotion of positive Information Governance culture which instils corporate and public confidence, building a credible reputation as a data controller.

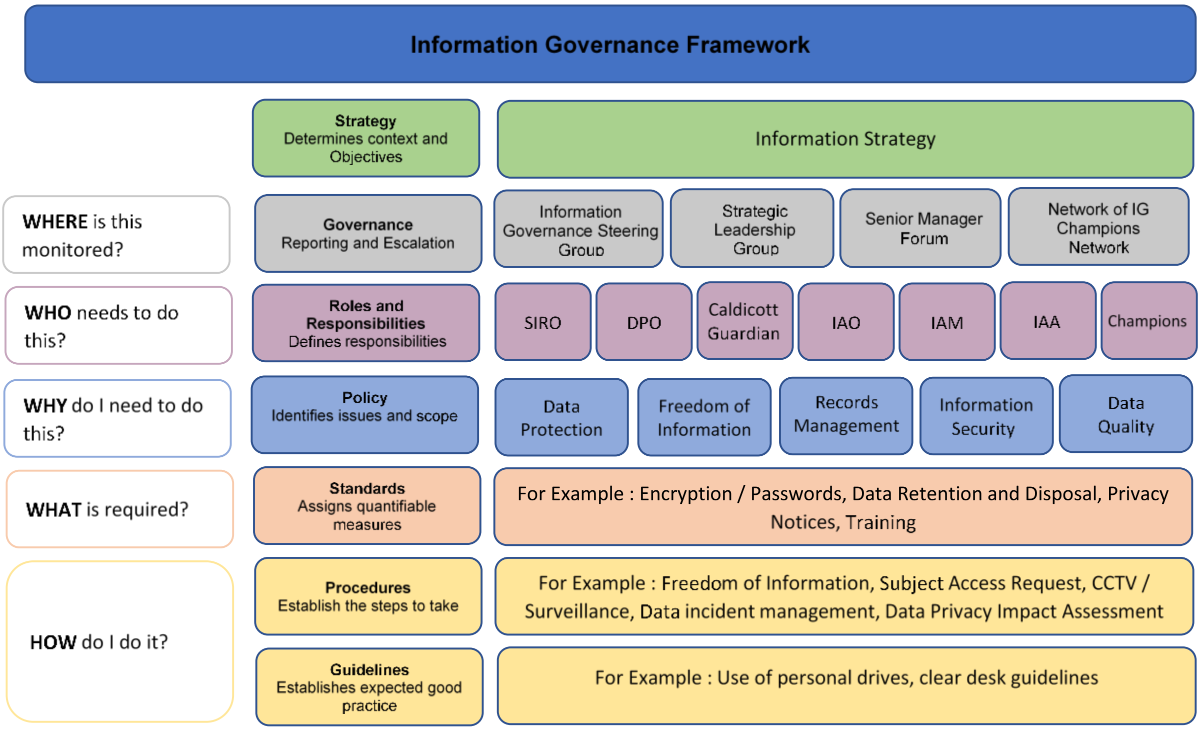
2.6 The Framework and the underpinning strategies are based upon the following standards and legislation that apply to information governance and management:

| | | | | |
|---|---|---|---|---|
| Data Protection Act 2018 | Health and Social Care Act 2012 | Freedom of Information Act 2000 | General Data Protection Regulation 2018 (GDPR); | 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 |
| Huiman Rights Act 1998 | Information Security NHS Code of Practice | Information Security Standard ISO 27002:2005 | Records Management code of Practice for Health and Social Care 2016 | Mental Capacity Act 2005 |
| NHS Constitution – Department of Health | NHS Data Security andProtection Toolkit (DSPT) | ICO guidance and good practice | Notification of Data Security and Protection incidents (May 2018) | Openness of Local Government Bodies Regulations 2014 |

## 3.0 Information Governance Framework

3.1 Information Governance is about ensuring that organisational information is managed as an asset to ensure that all statutory, regulatory and best practice requirements are met.

3.2 Our approach is set out in the diagram below:



**Information Governance Framework**

| | | |
|---|---|---|
| | **Strategy** Determines context and Objectives | Information Strategy |
| **WHERE** is this monitored? | **Governance** Reporting and Escalation | Information Governance Steering Group<br>Strategic Leadership Group<br>Senior Manager Forum<br>Network of IG Champions Network |
| **WHO** needs to do this? | **Roles and Responsibilities** Defines responsibilities | SIRO<br>DPO<br>Caldicott Guardian<br>IAO<br>IAM<br>IAA<br>Champions |
| **WHY** do I need to do this? | **Policy** Identifies issues and scope | Data Protection<br>Freedom of Information<br>Records Management<br>Information Security<br>Data Quality |
| **WHAT** is required? | **Standards** Assigns quantifiable measures | For Example : Encryption / Passwords, Data Retention and Disposal, Privacy Notices, Training |
| **HOW** do I do it? | **Procedures** Establish the steps to take | For Example : Freedom of Information, Subject Access Request, CCTV / Surveillance, Data incident management, Data Privacy Impact Assessment |
| | **Guidelines** Establishes expected good practice | For Example : Use of personal drives, clear desk guidelines |

3.3 All supporting policies, standards, procedures and guidelines will be made available through the shared drives and intranet.

## 4.0 Key Roles and Responsibilities

4.1 Information Governance is the responsibility of all employees and contractors working on behalf of the CCG and / or 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.

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

### Accountable Officer / Chief Executive

4.3 The Accountable Officer / Chief Executive has overall responsibility for Information Governance of both the Council and CCG, which includes the effective management through appropriate mechanisms which support service delivery and continuity.

### Senior Information Risk Officer (SIRO)

4.4 The SIRO 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.

4.5 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 agrees actions in respect of identified information risks; and
- ensures sufficient resources are in place to manage the information governance agenda.

### Data Protection Officer (DPO)

4.6 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).

4.7 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 the ICO.

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

4.9 There will be respective DPOs within both the CCG and Council. The CCG's DPO will, in addition, support General Practice in accordance with the standard GP contract requirements and management of conflicts of interest.

### Caldicott Guardian

4.10 The Caldicott Guardian is 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.

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

**Chief Information Officer (CIO)**

4.12 With the development of the digital agenda, greater emphasis has been incorporated into statutory requirements on Cyber and Data Security. The CIO oversees the arrangements in both organisations through either direct or commissioned provision for the security of networks, including remote working facilities and ensuring effective controls are in place.

**Information Governance Manager (IG Manager)**

4.13 The IG Manager is responsible for ensuring the day-to-day delivery of the Information Governance agenda, including oversight and delivery for all aspects of Data Security and Protection Toolkit.

4.14 The IG Manager will ensure that in addition to internal relationships with identified Information Governance post holders, they will also foster good relationships across Greater Manchester in respect of and specifically with the NHS Greater Manchester Information Governance Group (NHS GM IG Group) and the Greater Manchester Combined Authority (GMCA) Senior Information Governance Lead and ensure any regional guidance is reflected into local practice as necessary.

**Information Asset Owners**

4.15 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).

4.16 Deputy and / or Assistant Directors, or equivalent, have been identified as IAOs.

**Information Asset Managers**

4.17 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.

4.18 Heads of Service have been designated as IAMs

### Information Asset Administrators (Champions)

4.19 All employees and individuals working on behalf of the Council and / or CCG 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 risks, issues and concerns as they emerge. The IAAs are collectively responsible to achieving Information Governance success.

### Information Governance Champion

4.20 Each area will identify an Information Governance Champion (IGC), who will take an active role, working alongside the IAO, IAM and IAAs to ensure that the information governance agenda is enabled through day-to-day operations. The IGCs will be supported to increase their knowledge and understanding of information governance related activity and will act as a departmental expert and advocate for good information governance practice.

## 5.0 Governance and Reporting Arrangements

5.1 To support the delivery of the Information Governance Framework, two delivery groups will be established.

5.2 An Information Governance Steering Group (IGSG) will bring together strategic leads who support the Information Governance agenda, including the SIRO, designate SIRO, Data Protection Officer(s), Caldicott Guardian(s), CIO, IG Manager and other representatives from each department as required, 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

5.3 In addition, the Strategic Leadership Group (SLG) and Senior Manager Forum (SMF) will bring together the Information Asset Managers to ensure all operational aspects of information governance are progressed and compliant 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 Data Protection Impact Assessment (DPIA) and Data Sharing Agreement (DSA) registers;
- Oversee delivery of actions arising from data breaches;
- Provide updates on departmental performance in respect of Subject Access Requests (SARs) and Freedom of Information requests (FOIs); and
- Contribute to and prepare compliance reports with annual assessments and audits.

5.4 The IG Manager will also bring together the network of IGCs to support continued improvements in the wider application of Information Governance across all teams.

## 6.0 Dissemination, Implementation and Training

6.1 The framework will be communicated to all staff through corporate communication channels and will be mandated as part of every new starter induction, and periodically thereafter, in line with the corporate training standard for information governance, whether employed, elected, contracted or working on a voluntary basis.

6.2 A Training Needs Analysis will be completed annually, and all staff and Elected Members will receive training consummate with their roles and responsibilities around information handling, management and cyber security.

6.3 As a minimum, all staff are required to complete the mandatory Information Governance module using the agreed method detailed in the approved Training Needs Analysis, however further modules for specific information governance and / or certain business roles will be available through e-learning and / or classroom sessions, developed internally or through recognised providers, as required. The requirements and standards for these will be developed, agreed and kept under review.

6.4 The SIRO, Caldicott Guardian(s), DPO, IG Manager, IAOs and IAMs must complete relevant additional training.

6.5 Training compliance will be monitored by the IGSG and at an individual employee level through the annual appraisal process.

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

6.7 Regular reminders on information governance topics will be delivered through corporate and team briefings, staff newsletters and e-mail communication.

6.8 Failure to comply with Information Governance training requirements will be managed in accordance with agreed policies.

## 7.0 Monitoring and Review

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

7.2 The policies, procedures, standards and guidance that form part of the Framework will be reviewed as set out in the individual documents.

7.3 A detailed review and change log of all documents which comprise this Framework will be maintained by the Information Governance Manager.

## 8.0 Other related documents

8.1 This Framework should be read in conjunction with the suite of other Information Governance Policies, procedures and guidelines.