# A group of colorful circles with text Description automatically generatedInformation Governance Management Framework

|  |  |
| --- | --- |
| Complete the blank cells in the table below. The rest will be added by the corporate team once the policy approved and before it is added to the website. | |
| **Policy ref no:** |  |
| **Responsible Executive Director:** | Deb El-Sayed |
| **Author and Job Title:** | IG Team, South Central and West Commissioning Support Unit (SCW) |
| **Date Approved:** | 14th June 2024 |
| **Approved by:** | *Deb El-Sayed, SIRO and Information Governance Group* |
| **Date of next review:** | June 2026 |

## Policy Review Checklist

|  | **Yes/No/NA** | **Supporting information** |
| --- | --- | --- |
| Has an Equality Impact Assessment Screening been completed? | Yes |  |
| Has the review taken account of latest Guidance/Legislation? | Yes |  |
| Has legal advice been sought? | N/A |  |
| Has HR been consulted? | N/A |  |
| Have training issues been addressed? | Yes | Support is available via SCW CSU IG Consultant |
| Are there other HR related issues that need to be considered? | No |  |
| Has the policy been reviewed by Staff Partnership Forum? | N/A | This is not a framework related to HR |
| Are there financial issues and have they been addressed? | N/A |  |
| What engagement has there been with patients/members of the public in preparing this policy? | N/A |  |
| Are there linked policies and procedures? | Yes | This framework is the overarching document that governs the suite of IT/IG related documents which support the ICB’s responsibilities |
| Has the lead Executive Director approved the policy? | Yes | Senior Information Risk Owner (SIRO) |
| Which Committees have assured the policy? | N/A | Information Governance Group approve the framework |
| Has an implementation plan been provided? | Yes | See Implementation Plan |
| How will the policy be shared with | Yes | See Implementation Plan |
| Will an audit trail demonstrating receipt of policy by staff be required; how will this be done? | No |  |
| Has a DPIA been considered in regards to this policy? | N/A |  |
| Have Data Protection implications have been considered? | Yes | This document underpins compliance |

|  |  |  |
| --- | --- | --- |
| Version | Date | Consultation |
| 0.1 (1.0) | 14-09-2018 | New policy to align to GDPR |
| 1.1 | September 2020 | Review |
| 1.2 | December 2022 | Review |
| 1.3 | March 2023 | Review. Update Responsible Executive and amend from CCG to an ICB Policy |
| 1.4 | February 2024 | Review. Update minor cosmetic changes |
| 1.5 | June 2024 | Reference to strategy removed and EHIA completed |

# Table of contents

[Information Governance Management Framework 1](#_Toc176865360)

[Policy Review Checklist 2](#_Toc176865361)

[Table of contents 3](#_Toc176865362)

[Information Governance Management Framework 5](#_Toc176865363)

[1 Introduction 5](#_Toc176865364)

[1.1 BNSSG ICB Values 5](#_Toc176865365)

[2 Purpose and scope 5](#_Toc176865366)

[3 Duties – legal framework for this policy 6](#_Toc176865367)

[4 Responsibilities and Accountabilities 6](#_Toc176865368)

[5 Definitions/explanations of terms used 10](#_Toc176865369)

[6 Information Governance Principles 11](#_Toc176865370)

[7 Training requirements 12](#_Toc176865371)

[8 Equality Impact Assessment 12](#_Toc176865372)

[9 Implementation and Monitoring Compliance and Effectiveness 12](#_Toc176865373)

[10 Countering Fraud, Bribery and Corruption 13](#_Toc176865374)

[11 References, acknowledgements and associated documents 13](#_Toc176865375)

[12 Appendices 14](#_Toc176865376)

[12.1 Legislation 14](#_Toc176865377)

[12.3 Equality and Health Inequality Impact Assessment (EHIA) 15](#_Toc176865378)

[13. Implementation Plan 16](#_Toc176865379)

# Information Governance Management Framework

## Introduction

Information Governance (IG) is the framework for handling information in a secure and confidential manner that allows organisations and individuals to manage patient, personal and sensitive information legally, securely, efficiently and effectively in order to deliver the best possible healthcare and services.

This framework sets out the approach taken by Bristol, North Somerset and South Gloucestershire Integrated Care Board (BNSSG ICB) for embedding information governance and details the continuous improvements that the ICB is working towards. The organisation must have a robust information governance management framework to provide the clarity and context for its information governance activities.

The framework identifies how the ICB will deliver its strategic information governance responsibilities by identifying the accountability structure, processes, interrelated policies, procedures, improvement plans, reporting hierarchy and training within the ICB. The ICB will also ensure that the future management and protection of organisational information is in compliance with legislative and government process and procedure including the National Data Guardian’s 10 Data Security Standards.

This information governance management framework document is aligned with BNSSG ICBs objective to support the delivery of ICB operating and strategic plan.

### BNSSG ICB Values

This information governance management framework document is aligned with ICB values, in particular:

*We act with integrity* – compliance with Data Protection Legislation requires the ICB to be open and transparent in our use of personal information this supports the creation of a culture of trust and respect.

*We do the right thing* – this Framework supports the ICB’s legal compliance and aims to ensure that all activities are aligned to Data Protection legislation.

## Purpose and scope

This document applies to all directly and indirectly employed staff within the ICB and other persons working within or on behalf of the organisation. This document applies to all third-party contractors or those with similar relationships through their contractual agreement to carry out activities on behalf of the ICB.

‘Information governance’ describes the approach taken within which information standards are developed, implemented, and maintained by the ICB. Information governance ensures best practice is applied to all information relating to the organisation and individuals.

Information governance management ensures that data is sourced, held, and used legally, securely, efficiently and effectively, to deliver the best possible care and services in compliance with legislation and advice received from bodies including NHS England. Information is a vital asset to the organisation supporting the effective management of commissioned services and resources. Therefore, it is essential that all organisational information be managed effectively within a robust information governance management framework.

The organisation requires accurate, timely and relevant information to enable it to commission the highest quality healthcare and to operate effectively and meet its objectives. It is the responsibility of all staff to ensure that information is accurate and current and is used proactively in the conduct of its business. Accurate information that is dependable plays a key role in both corporate and clinical governance, strategic risk, performance management and service planning.

The implementation of this framework will lead to improvements in information handling underpinned by clear standards. The ICB will be able to ensure that all employees manage personal information in compliance with NHS England regulations for governance.

Staff will be aware that their records will not be disclosed inappropriately, which will lead to greater confidence in NHS working practices.

The information governance framework should be seen as a tool that will aid the ICB in preparation for embedding a ‘robust governance framework’. Information governance contributes to other standards by ensuring that data required for supporting decisions, processes and procedures are accurate, available and endures.

This framework is augmented by other related documents including those listed in Section 10 below.

## Duties – legal framework for this policy

BNSSG ICB is legally responsible for compliance with UK Data Protection Legislation.

## Responsibilities and Accountabilities

**4.1 Chief Executive**

The Chief Executive has overall responsibility for Information Governance legislation and best practices, and the requirements within the ‘Data Security and Protection Toolkit’ (DSPT) within the organisation. They are responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity. The management of information risk and information governance practice is required within the Statement of Internal Control which the Accountable Officer is required to sign annually.

**4.2 Senior Information Risk Owner (SIRO) – Chief Transformation, Data and Digital Officer/Chief Digital Information Officer**

The Senior Information Risk Owner for the ICB is the Chief Transformation, Data, and Digital Officer/Chief Digital Information Officer, an executive board member with allocated lead responsibility for the organisation’s information risks and provides the focus for management of information risk at executive management level. The Chief Executive must receive assurances from the SIRO that information risk is being managed suitably and successfully throughout the ICB, and for any services contracted by the organisation. The Caldicott Guardian, the Data Protection Officer, the IG Manager (SCW), and the Information Asset Owners (IAOs) provide support to the SIRO.

**4.3. The Caldicott Guardian (CG) – Chief Medical Officer**

The Caldicott Guardian is a member of the Executive Management Team and a senior health or social care professional with responsibility for promoting clinical governance or equivalent functions and advising on confidentiality issues. The Caldicott Guardian acting as the conscience of the organisation plays a key role in ensuring that the ICB satisfies the highest practical standards for handling patient/staff identifiable information. The Caldicott Guardian serves as part of a broader Caldicott function and is supported by the Data Protection Officer and SCW Information Governance Team.

**4.4. Data Protection Officer (DPO)**

The Data Protection Officer (DPO) will report directly to the Governing Body in matters relating to data protection assurance and compliance, without prior oversight by their line manager.

The DPO must ensure that their responsibilities are not influenced in anyway and should a potential conflict of interest arise report this to the highest management level.

The DPOs cannot hold a position within the organisation that can be considered a key decision maker in relation to what personal data is collected and used. Their primary duties are to

* Inform and advise organisation and staff of their IG responsibilities
* Monitor compliance with the UK GDPR and the DPA 2018
* Provide advice where requested regarding the Data Protection Impact Assessment, and monitor performance
* Cooperate with the supervisory authority
* Be the principal contact point with the Information Commissioners Office – in particular for incidents

They must give due regard to the risks associated with the processing of data undertaken by the organisation and work with the SIRO and Caldicott Guardian to achieve this.

The Data Protection Officer (DPO) is the person within the ICB that will ensure that Information Governance incidents which are likely to result in a risk to the rights and freedoms of individuals the ICO (Information Commissioner’s Office) is informed within 72 hours. They are also part of the Data Protection Impact Assessment (DPIA) process.

**4.5. Information Asset Owners (IAO’s)**

The SIRO is supported by Information Asset Owners (IAOs). The role of the IAO is to understand what information is held, what is added and what is removed, who has access and why in their own area. As a result, they are able to understand and address risks to the information assets they ‘own’ and to provide assurance to the SIRO that information risks within their areas of responsibilities are identified, recorded and that controls are in place to mitigate those risks. They will also investigate and take action on any potential breaches of the organisations policies and procedures and ensure that a Data Protection Impact Assessment (DPIA) is undertaken where appropriate.

**4.6.**

**Information Asset Administrators (IAAs)**

Information Asset Administrators are required to support the IAO’s and SIRO who will work with the Information Governance Team to ensure staff apply the data protection legislation and Caldicott Principles within daily working practices.

IAAs serve as local records managers and are responsible for assisting in the co-ordination of all aspects of information governance requests in the execution of their duties, which include:

* provide support to their IAO
* ensure that policies and procedures are followed locally
* recognise potential or actual IG security incidents
* undertake relevant IG audit tasks
* consult their IAO on incident management
* ensure that information asset registers are accurate and maintained up to date
* **.**

**4.7. SCW Information Governance Service**

SCW provides IG support services in line with the information governance service specification under any Service Level Agreement for IG Service.

**4.8. The BNSSG Information Governance Group (IGG)**

The Information Governance Group (IGG) oversees and provides leadership within BNSSG ICB for Information Governance (IG), ensuring that it complies with statutory responsibilities and fulfils the requirements of data protection legislation, the common law duty of confidentiality and The Records Management Code of Practice for Health and Social Care Act 2012.

As stated in the Terms of Reference IGG is responsible:

* To provide a forum for the scrutiny of the IG management framework and assurance model.
* To oversee the annual IG assessment for sign off by the ICB.
* To agree and oversee the organisation’s IG improvement programme.
* To ensure that the organisation’s approach to IG is communicated to all staff and made available to the public as appropriate.
* To offer support, advice and guidance to the Caldicott Function and Data Protection programme within the organisation.
* To monitor the organisation’s information handling activities to ensure compliance with law and guidance.
* To ensure that training made available by the organisation is taken up by staff as necessary to support their role.
* To ensure that corporate records management standards are developed and implemented within the organisation.
* Provide a focal point for the resolution and/or discussion of IG issues.
* Review the flows of information to ensure they are appropriate and supported by relevant documentation especially those involving any transfer of personal data.
* To ensure that all new developments undertake statutorily required Data Protection Impact Assessments (DPIAs) to assess IG implications where required.
* To ensure that Continuity plans for services include appropriate reference to information assets and continuity/recovery activities.
* To support the work of the SIRO, DPO, Caldicott Guardian (CG), Information Asset Owners (IAO) and Information Asset Administrators (IAA).
* To review all information and information security incidents.
* Review information and information security risks/issues and to escalate where appropriate within the organisation and with customers.
* To ensure a comprehensive suite of IG policies is in place.
* To receive and review DSP toolkit project/action plans.
* To act as the ICB sub-licensing approval Group, ensuring the necessary assurance, controls and measures are in place before approval is granted to data.

A quarterly IG report shall be presented to the IGG. Audit Committee will receive minimum annual updates onprogress, information governance audits, training and toolkit evidence requirements, together with updates on any incidents that may have occurred.

The annual audit of information governance shall be reported to the Audit Committee via IGG together with any recommendations identified and the associated improvement plans.

Risks and issues will be identified where they may impact upon delivery of the IG improvement programme or the DSPT submission which will be monitored by the IGG.

**4.9. The BNSSG IAO/IAA Group**

The Information Asset Owners and Information Asset Administrators Group has been established to enable the IAO’s and IAA’s to receive vital information in order to assist in the implementation and assure compliance with the Information Governance (IG) agenda for the ICB.

It is chaired by the SCW IG Consultant on behalf of the SIRO by SCW Information Governance Consultant and provides a forum to enable a pro-active environment for the exchange of information. It will provide a platform to debate and discuss areas of concern where difficulties are experienced requiring mitigation, and to exchange good practice.

## Definitions/explanations of terms used

In order to assist staff with understanding their responsibilities under this framework, the following types of information and their definitions are applicable in all ICB policies and documents:

|  |  |
| --- | --- |
| **Personal Data**  (derived from the UK GDPR) | Any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person |
| **‘Special Categories’ of Personal Data**  (derived from the UK GDPR) | ‘Special Categories’ of Personal Data is different from Personal Data and consists of information relating to:   1. The racial or ethnic origin of the data subject 2. Their political opinions 3. Their religious beliefs or other beliefs of a similar nature 4. Whether a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1998 5. Genetic data 6. Biometric data for the purpose of uniquely identifying a natural person 7. Their physical or mental health or condition 8. Their sexual life |
| **Personal Confidential Data** | Personal and Special Categories of Personal Data owed a duty of confidentiality (under the common law). This term describes personal information about identified or identifiable individuals, which should be kept private or secret. The definition includes dead as well as living people and ‘confidential’ includes information ‘given in confidence’ and ‘that which is owed a duty of confidence’. The term is used in the Caldicott 2 Review: Information: to share or not to share (published March 2013). |
| **Commercially confidential Information** | Business/Commercial information, including that subject to statutory or regulatory obligations, which may be damaging to SCW CSU or a commercial partner if improperly accessed or shared. Also as defined in the Freedom of Information Act 2000 and the Environmental Information Regulations 2004. |

## Information Governance Principles

Implementation of robust information governance arrangements will deliver improvements in information handling by following the Department of Health standards (known as the ‘HORUS’ model), these standards require that information will be:

**H**eld securely and confidentially

**O**btained fairly and efficiently

**R**ecorded accurately and reliably

**U**sed effectively and ethically

**S**hared appropriately and lawfully

Information governance provides consistency and best practice for the many different information handling activities. These principles are equally supported by the Caldicott Principles which have been subsumed into the NHS Code of Confidentiality.

There are five interlinked principles, which serve to guide these information governance responsibilities:

* Openness
* Legal compliance
* Information security
* Quality assurance
* Proactive use of information

## Training requirements

It is the responsibility of the ICB to ensure that all new staff are provided with information governance, information security, freedom of information and records management training as part of their induction. Induction training is to be completed within 1 month of joining the organisation. All new staff as part of their induction must use ConsultOD to access their NHS Digital Data Security and Awareness training, Data Security Awareness and Information Governance Handbook and the ICBs Acceptable Use Policy. Refresher training will/must be completed through the above tool or where appropriate and agreed via training provided by the IG Team on an annual basis.

The ICB, through its learning and development commitment ensures that appropriate annual training is made available to staff and completed as necessary to support their duties. In addition to the annual mandatory training all IAOs, IAAs, the DPO, the Caldicott Guardian and SIRO are required to have undertaken all of their additional training associated with their identified framework roles as identified in the ICBs training needs analysis. A TNA will be produced for agreement by IGG to govern training requirements.

**Supporting People**

Fundamental to the success of delivering the information governance framework is developing a robust information governance culture within the ICB. In order to promote this culture, training needs to be relevant and embedded in working practices. Through the provision of IG services by SCW the IG manager is actively involved in this development through the provision of assistance on specific projects and issues, investigations and the development of remedial action plans and the ongoing provision of relevant information and reminders.

Following a Serious Incident Requiring Investigation (SIRI) further training may be delivered as a mandatory requirement where an incident has occurred, as deemed appropriate as part of the investigation findings. Disciplinary procedures may be used where it is proven that an employee has acted in breach of the terms of their contract; acts of gross misconduct will lead to dismissal.

## Equality Impact Assessment

EIA Screening in Appendix \*\*\*.

## Implementation and Monitoring Compliance and Effectiveness

The performance of the framework will be monitored in two ways:

* Against the criteria set in the Data Security and Protection Toolkit, using the annual submission on 31 June and associated improvement plan.
* The internal audit process and subsequent report to the audit committee.

## Countering Fraud, Bribery and Corruption

The ICB is committed to reducing and preventing fraud, bribery and corruption in the NHS and ensuring that funds stolen by these means are put back into patient care. During the development of this policy document, we have given consideration to how fraud, bribery or corruption may occur in this area. We have ensured that our processes will assist in preventing, detecting and deterring fraud, bribery and corruption and considered what our responses to allegation of incidents of any such acts would be.

In the event that fraud, bribery or corruption is reasonably suspected, and in accordance with the Local Counter Fraud, Bribery and Corruption Policy, the ICB Team will refer the matter to the ICB’s Local Counter Fraud Specialist for investigation and reserve the right to prosecute where fraud, bribery or corruption is suspected to have taken place. In cases involving any type of loss (financial or other), the ICB will take action to recover those losses by working with law enforcement agencies and investigators in both criminal and/or civil courts.

## References, acknowledgements and associated documents

This management framework links to other strategies, policies, procedures and legislation/codes of practice (See Appendix 13.3) that are in place within the ICB to promote and ensure the delivery of information governance standards throughout the organisation, including but not limited to those documents listed below.

T

## Appendices

### Legislation

All staff are required to comply with Data Protection Legislation. This includes:

* the UK General Data Protection Regulation (GDPR),
* the Data Protection Act (DPA) 2018,
* the Law Enforcement Directive (Directive (EU) 2016/680) (LED) and any applicable national Laws implementing them as amended from time to time

In addition, consideration will also be given to all applicable Law concerning privacy confidentiality, the processing and sharing of personal data including

* the Human Rights Act 1998,
* the Health and Social Care Act 2012 as amended by the Health and Social Care (Safety and Quality) Act 2015,
* the common law duty of confidentiality and
* the Privacy and Electronic Communications (EC Directive) Regulations 2003

Consideration must also be given to the

* Computer Misuse Act 1990 and as amended by the Police and Justice Act 2006 (Computer Misuse)
* Copyright, Designs and Patents Act 1988
* Regulation of Investigatory Powers Act 2000
* Electronic Communications Act 2000
* Freedom of Information Act 2000
* Other relevant Health and Social Care Acts
* Access to Health Records Act 1990
* Fraud Act 2006
* Bribery Act 2010
* Criminal Justice and Immigration Act 2008
* Equality Act 2010
* Terrorism Act 2006
* Malicious Communications Act 1988
* Counter-Terrorism and Security Act 2015
* Digital Economy Act 2010 and 2017

**GUIDANCE**

* [ICO Guidance](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/)
* [CQC Code of Practice on Confidential Information](https://www.cqc.org.uk/sites/default/files/20180419%20Code%20of%20practice%20on%20CPI%20with%20GDPR%20and%20IRMER%20updates.pdf)
* [Looking after information - NHS Digital](https://digital.nhs.uk/data-and-information/looking-after-information)
* [NHS England » Confidentiality Policy](https://www.england.nhs.uk/publication/confidentiality-policy/)
* [Records management: code of practice for health and social care - GOV.UK](https://www.gov.uk/government/publications/records-management-code-of-practice-for-health-and-social-care)
* [Confidentiality: NHS Code of Practice - Publications - Inside Government - GOV.UK](https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice)
* [Confidentiality: NHS Code of Practice - supplementary guidance](https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice-supplementary-guidance-public-interest-disclosures)
* [Installing CCTV? Things you need to do first | ICO](https://ico.org.uk/for-organisations/sme-web-hub/whats-new/blogs/installing-cctv-things-you-need-to-do-first/)

### 12.3 Equality and Health Inequality Impact Assessment (EHIA)



## 13. Implementation Plan

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Target Group** | **Implementation or Training objective** | **Method** | **Lead** | **Target start date** | **Target End date** | **Resources Required** |
| All staff | The Voice | Request content included | AG | Sept 2024 | Sept 2024 | None |
| All staff | To ensure document is available | The Hub | AG | Aug 2024 | Aug 2024 | None |
| IAO/IAA | Awareness | IAO/IAA Meeting | AG | Sept 2024 | Sept 2024 |  |
|  |  |  |  |  |  |  |