 

# Information Governance Policy



1

|  |
| --- |
| **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:** | 10 |
| **Responsible Executive Director:** | Deborah El-Sayed |
| **Author and Job Title:** | **Information Governance Team, SCW CSU** |
| **Date Approved:** | 25th November 2024 |
| **Approved by:** | Shane Devlin, Chief Executive |
| **Date of next review:** | November 2026 |

## Policy Review Checklist

|  |  |  |
| --- | --- | --- |
|  | **Yes/No/NA** | **Supporting information** |
| Has an Equality Impact Assessment Screening been completed? | Yes | See attached |
| Has the review taken account of latest Guidance/Legislation? | Yes |  |
| Has legal advice been sought? | No | Policy template provided by SCW CSU IG Team |
| Has HR been consulted? | Yes | Via CPRG |
| Have training issues been addressed? | No |  |
| Are there other HR related issues that need to be considered? | No |  |
| Has the policy been reviewed by Staff Partnership Forum? | No |  |
| Are there financial issues and have they been addressed? | No |  |
| What engagement has there been with patients/members of the public in preparing this policy? | N/A |  |
| Are there linked policies and procedures? | Yes | IG Policy suite |
| Has the lead Executive Director approved the policy? | Yes | Via IGG |
| Which Committees have assured the policy? | Yes | IGG |
| Has an implementation plan been provided? | Yes |  |
| How will the policy be shared with | Yes | Intranet |
| 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 |  |

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Consultation** |
| 1.2 | June 2022 | Approved |
| 1.3 | June 2024 | Minor changes |
| 1.4 | October 2024 | Requirements to add reference to managed services and reference to Directorate leads role following IGG review and approval. |

# Table of contents

[Information Governance Policy 1](#_bookmark0)

[Policy Review Checklist 2](#_bookmark1)

[Table of contents 4](#_bookmark2)

[Information Governance Policy 5](#_bookmark3)

1. [Introduction 5](#_bookmark4)
	1. [BNSSG ICB Values 5](#_bookmark5)
2. [Purpose and scope 5](#_bookmark6)
3. [Duties – legal framework for this policy 6](#_bookmark7)
4. [Responsibilities and Accountabilities 7](#_bookmark8)
5. [Definitions/explanations of terms used 9](#_bookmark9)
6. [Information Governance 10](#_bookmark10)
7. [Information Quality Assurance 11](#_bookmark11)
8. [Commissioning of new services and the use of data protection impact assessments](#_bookmark12) [11](#_bookmark12)
9. [Training requirements 12](#_bookmark13)
10. [Equality Impact Assessment 12](#_bookmark14)
11. [Implementation and Monitoring Compliance and Effectiveness 12](#_bookmark15)
12. [Countering Fraud, Bribery and Corruption 12](#_bookmark16)
13. [References, acknowledgements and associated documents 13](#_bookmark17)
14. [Appendices 13](#_bookmark18)
	1. [Equality Impact Assessment 13](#_bookmark19)
	2. [Implementation Plan 14](#_bookmark20)

# Information Governance Policy

## Introduction

The role of the ICB is to support the commissioning of healthcare, both directly and indirectly, so that valuable public resources secure the best possible outcomes for patients. This policy will support the ICB’s compliance with data protection legislation and will help ensure that the people who work for the ICB understand how to look after the information they need and use to do their jobs, to protect this information on behalf of patients and to support legal compliance.

### BNSSG ICB Values

The Information Governance Policy sets out the ICBs position regarding ensuring compliance with data protection legislation this demonstrates the ICB striving for excellence and to doing the right thing with regard to how confidential information is managed.

## Purpose and scope

This document is derived from and supports the Information Governance Policy published by NHS England, the scope of which includes those working for Integrated Care Boards (ICBs).

Information is a vital asset. It plays a key part in ensuring the efficient management of service planning, resources and performance management. It is therefore of paramount importance to ensure that information is efficiently managed, and that appropriate policies, procedures and management accountability and structures provide a robust governance framework for information management for all systems and services including hosted systems (e.g Federated Data Platform and the South West Secure Data Envirnoment).

Information Governance looks at the way the NHS handles information about patients, staff, contractors and the healthcare provided, with particular consideration of personal and confidential information. Without access to information, it would be impossible to provide quality healthcare and good corporate governance. A robust governance framework needs to be in place to manage this vital asset, providing a consistent way to deal with the many different information handling requirements including:

* Information Governance Management
* Confidentiality and Data Protection Legislation assurance
* Corporate Information assurance
* Information Security assurance
* Secondary Use assurance

The aims of this policy are to maximise the value of organisational assets by ensuring that information is:

* Held securely and confidentially
* Obtained fairly and efficiently
* Recorded accurately and reliably
* Used effectively and ethically
* Shared appropriately and lawfully

To protect the organisation’s information assets from all threats, whether internal or external, deliberate or accidental, the ICB will ensure that:

* Information will be protected against unauthorised access
* Confidentiality of information will be assured
* Integrity of information will be maintained
* Information will be supported by the highest quality data
* Regulatory and legislative requirements will be met
* Business continuity plans will be produced, maintained and tested
* Information Governance, Information security/cyber training will be available to all staff The scope of this document covers:
* All permanent employees of the ICB and;
* Staff working on behalf of the ICB (this includes contractors, temporary staff, and secondees).

The ICB recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. The ICB fully supports the principles of corporate governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard information. The ICB also recognises the need to share information in a controlled manner. The ICB believes that accurate, timely and relevant information is essential to deliver the highest quality health care. As such it is the responsibility of managers and staff to ensure and promote the quality of information and to actively use information in decision making processes.

## Duties – legal framework for this policy

The ICB regards all identifiable personal information as confidential except where national policy on accountability and openness requires otherwise.

The ICB will maintain policies to ensure compliance with Data Protection Legislation. This includes the UK General Data Protection Regulation (UK 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.

The ICB, when acting as a Controller, will identify and record a condition for processing, as identified by the UK GDPR under Articles 6 and 9 (where appropriate), for each activity it undertakes. When relying on Article 6, 1 (e) ‘processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller’, the ICB will identify the official authority (legal basis) and record this on relevant records of processing.

## Responsibilities and Accountabilities

#### Executive Management Team

It is the role of the ICB Executive Management Team to define the ICBICB policy in respect of Information Governance, considering legislative and NHS requirements. The Executive Management Team is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

#### 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.

#### Chief Executive

The ICB Chief Executive has overall responsibility for Information Governance 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 now required within the Statement of Internal Control which the Accountable Officer is required to sign annually.

#### Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner for the ICB is 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. The SCW Information Governance Manager will support the SIRO in fulfilling this role. In the absence of the SIRO there is a Deputy SIRO.

#### Caldicott Guardian

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.

#### Data Protection Officer

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.

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.

#### Directorate Information Governance Lead

The Directorate Information Governance Lead role is a senior member of staff who has been identified to represent a ICB Directorate and has responsibility for Directorate compliance to Information Governance processes. This includes being a member of the ICB Information Governance Group and providing support for the requirements of the Data Protection and Security Toolkit.

#### Information Asset Owners (IAO)

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.

#### Information Asset Administrators (IAA’s)

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

#### SCW Information Governance Manager

The SCW Information Governance Team supports the ICB and is responsible for ensuring that the Information Governance programme is implemented throughout the organisation. The team is also responsible for the completion and annual submission of the Data Security and Protection Toolkit. The Information Governance Team will support the organisation in investigating Serious IG Incidents Requiring Investigation (SIRIs), offer advice and support for the organisation to comply with legislation, policies and protocols as per the Service Level Agreement.

#### Management

All managers are responsible for promoting good information governance within their team. This includes ensuring that staff members complete relevant induction training and annual Data Security and Awareness training. Managers must also support Information Asset Owners in their activities and identify any new or changes processes that require a Data Protection Impact Assessment.

#### All staff

All staff have responsibility for complying with this policy and with Data Protection Legislation and for completing annual Data Security and Awareness training.

## Definitions/explanations of terms used

In order to assist staff with understanding their responsibilities under this policy, the following types of information and their definitions are applicable in all relevant 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:* The racial or ethnic origin of the data subject
* Their political opinions
* Their religious beliefs or other beliefs of a similar nature
* Whether a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1998
* Genetic data
* Biometric data for the purpose of uniquely identifying a natural person
* Their physical or mental health or condition
* 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. |

## Information Governance

* The ICB will ensure that it meets its national requirements in respect of its submission of the annual self-assessment Data Security and Protection Toolkit (DSPT).
* Non-confidential information about the ICB and its services will be available to the public through a variety of media.
* The ICB will maintain policies to ensure compliance with the Freedom of Information Act. Please refer to the Freedom of Information Policy.
* The ICB will maintain clear procedures and arrangements for handling requests for information from the public. Please refer to the Individual Rights Policy in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act (DPA) 2018.
* The ICB will maintain fair processing information and ensure that privacy notices are available to staff and member of the public as required.
* The ICB will maintain policies to ensure compliance with the Records Management Code of Practice for Health and Social Care (2016). Please refer to The Records Management Policy.
* The ICB will maintain policies for the effective and secure management of its information assets and resources.
* The ICB will promote effective confidentiality and security practice to its staff through policies, procedures and training.
* The ICB will adhere to the NHS Guidance for reporting, managing and investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation (IG SIRI) and as part of this, will review and maintain incident reporting procedures and monitor and investigate all reported instances of actual or potential breaches. Under Data Protection Legislation, where an incident is likely to result in a risk to the rights and freedoms of the Data Subject/individuals the Information Commissioner’s Office (ICO) must be informed no later than 72 hours after the organisation becomes aware of the incident.

## Information Quality Assurance

* The ICB will maintain policies and procedures for information quality assurance and the effective management of records.
* The ICB will undertake or commission annual assessments and audits of its information quality and records management arrangements.
* Managers are expected to take ownership of, and seek to improve, the quality of information within their services.
* Wherever possible, information quality should be assured at the point of collection.
* Data standards will be set through clear and consistent definition of data items, in accordance with national standards.

## Commissioning of new services and the use of data protection impact assessments

* The Data Protection Officer should be consulted during the design phase of any new service, process or information asset and contribute to the statutory Data Protection Impact Assessment (DPIA) process when new processing of personal data or special categories of personal data is being considered. Responsibilities and procedures for the management and operation of all information assets should be defined and agreed by the ICB SIRO and the Information Asset Owner’s.
* All staff members who may be responsible for introducing changes to services, processes or information assets must be effectively informed about the requirement to complete a statutory DPIA and where required, seek review from the SCW IG Manager prior to approval or further work.
* The ICB will maintain a DPIA framework that includes an approved template, guidance and supporting checklists.

## Training requirements

All new starters to the ICB inclusive of temporary, bank staff and contractors must undertake Information Governance induction training and provide acceptance of the Acceptable Use Policy and Information Governance staff handbook via the ConsultOD portal, to evidence compliance with the Data Protection Legislation and the DSP Toolkit assertions as part of the induction process. Extra training will be given to those dealing with requests for information. A register will be maintained of all staff who have completed the online training and those who have attended face to face training sessions where these are offered.

Annual IG training should be undertaken by all staff via the ConsultOD portal or face to face training.

## Equality Impact Assessment

See appendix 14.

## Implementation and Monitoring Compliance and Effectiveness

This policy will be monitored by SCW IG Team and the IGG to ensure any legislative changes that occur before the review date are incorporated.

The ICB will ensure that information governance is part of its annual cycle of internal audit. The results of audits will be reported to the ICB Information Governance Steering Group along with relevant action plans which they will monitor.

Compliance with the ICB policies is stipulated in staff contracts of employment. If staff members are unable to follow the ICB policies or the policy requirements cannot be applied in a specific set of circumstances, this must be immediately reported to the Line Manager, who should take appropriate action. Any non-compliance with the ICB policies or failure to report non-compliance may be treated as a disciplinary offence.

## 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 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

* NHS Digital Codes of Practice

<https://digital.nhs.uk/codes-of-practice-handling-information/confidential-information>

* Department of Health Code of Practice <https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice>
* Health and Social Care (Safety and Quality) Act 2015 <http://www.legislation.gov.uk/ukpga/2015/28/contents/enacted>
* NHS England Policy <https://www.england.nhs.uk/publication/confidentiality-policy/>
* All the Policies, procedures and guidance relating to the management and processing of information within the organisation including:
* Records Management Policy
* Freedom of Information and SARs Policy
* Confidentiality and Security of Information Policy
* Incident Reporting Policy
* Data Protection Act 2018
* UK General Data Protection Regulation

## Appendices

### Equality Impact Assessment



EHIA for IG Policy.pdf

### Implementation Plan

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Target Group** | **Implementation or Training objective** | **Method** | **Lead** | **Target start date** | **Target End date** | **Resources Required** |
| Staff | To have Policy available to staff | To be published on the Hub | Com ms/IG | Dec 2024 | Dec 2024 | Comms Team |
| Staff | To ensure all staff are aware of the Policy | To include in The Voice | Com ms/IG | Dec 2024 | Dec 2024 | Comms Team |
| Staff | To ensure all staff are aware of the Policy | To be sent to all IAO/IAAs | IG | Dec 2024 | Dec 2024 | N/A |