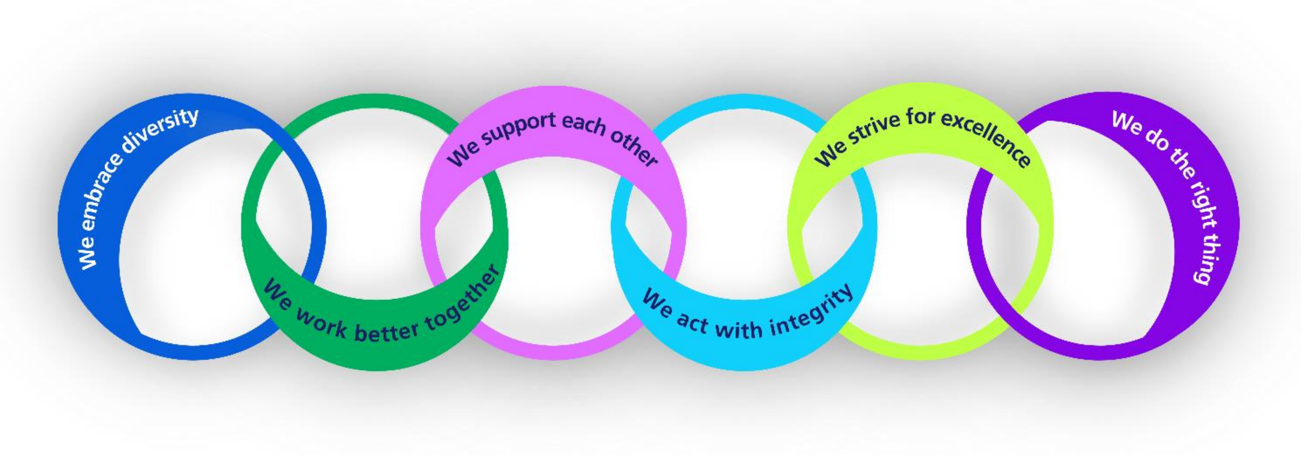
Healthier Together
Improving health and care in Bristol, North Somerset and South Gloucestershire

NHS
Bristol, North Somerset and South Gloucestershire
Integrated Care Board

Information Risk Management Process



Together we are BNSSG

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:	Deborah El-Sayed
Author and Job Title:	Caroline Dominey Strange and Alison Gane, South Central and West Commissioning Support Unit (SCW CSU) Information Governance Consultants
Date Approved:	June 2024
Approved by:	BNSSG ICB 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	See appendix
Has the review taken account of latest Guidance/Legislation?	Yes	
Has legal advice been sought?	N/A	
Has HR been consulted?	No	
Have training issues been addressed?	Yes	
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 process related to HR
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	This process is one of a suite of IT/IG related documents which support the ICBs responsibilities
Has the lead Executive Director approved the policy?	Yes	Via the Information Governance Group (IGG)
Which Committees have assured the policy?	N/A	Information Governance Group (IGG)
Has an implementation plan been provided?	Yes	See Appendix
How will the policy be shared with	N/A	Via The Hub
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	

	Yes/No/NA	Supporting information
Have Data Protection implications have been considered?	Yes	This process is part of a suite of documents that underpins Data Protection compliance

Version	Date	Consultation
1.1	Feb 2024	Annual review no legislative changes. Cosmetic changes and amendment from CCG to ICB
1.2	June 2024	Incorporate comments from IGG – add appendix SOP for Data Security and Protection Incident Management

Table of contents

Information Risk Management Process

1 Introduction

Information is a vital asset and is integral to governance, service planning and delivery, and performance management. To help ensure the safety and security of information within the organisation it is essential that information risk management is not considered in isolation but embedded into all business processes and functions.

Risk management is the recognition and effective management of all threats and opportunities that may have an impact on the organisation's reputation, its ability to deliver its statutory responsibilities and the achievement of its objectives and values.

It is critical that information risk be managed in a structured and robust way across all departments, with each department taking responsibility for information risk. Assets must be identified and ownership at senior staff level assigned. The basis of this approach is documented within the organisation's Information Governance Framework. This document must be read in conjunction with the following policies:

- Information Governance Policy
- Acceptable Use policy
- Records Management Policy

1.1 BNSSG ICB Values

Ensuring that we and protect information and manage information risks ensures the confidentiality, integrity and availability of the information that we rely on. This support our core values of being able to act with integrity, work better together and to do the right thing.

2 Purpose and scope

2.1 Purpose

The purpose of this document is to establish relevant lines of responsibility and conduct for all members of staff regarding information risk management. There are many types of information which require risk management including: personal information regarding staff and patients; commercially sensitive contracts and negotiations; procurement information.

As part of the organisation’s overarching information governance framework and policy, the Information Risk Management Process supports BNSSG ICB in ensuring that:

- Information is protected against unauthorised access
- Confidentiality of information is assured
- Integrity of information is maintained
- Regulatory requirements and legislation are met
- ICT systems are used in such a way as to prevent the unauthorised disclosure, destruction or modification of information and the integrity of all systems are maintained
- Strict access controls are applied to ensure that information, in whatever form, can only be accessed by those authorised to see it
- All breaches of information security, actual or suspected, are reported to, investigated and reported using the ICB’s Incident Management and Reporting Procedures and Standard Operating Procedure for managing Data Breaches.
- Information Governance training, called Data Security Awareness, ICBs Acceptable Use Policy and Data Security and Information Governance Staff handbook is available to all staff via the Consult OD website.

2.2 Scope

This document applies to all staff (which include temporary staff, contractors and seconded staff) and external staff/organisations providing services to the organisation by way of a Service Specification or other agreement.

This process will be reviewed every two years or where required more frequently.

3 Duties – legal framework for this policy

The ICB has a responsibility for ensuring that it meets its corporate and legal responsibilities and for the adoption of internal and external governance requirements. The ICB Executive Directors are responsible for ensuring that sufficient resources are available to support the requirements of information risk management within directorates.

4 Responsibilities and Accountabilities

4.1 Senior Information Risk Owner (SIRO)

The SIRO 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 SIRO will act as advocate for information risk for the organisation.

The SIRO has responsibility to:

- Take ownership of the information risk assessment and information risk management process
- Review and agree actions in respect of identified information risks
- Ensure that the organisational approach to information risk is effective in terms of resource, commitment and execution and that it is communicated to all staff
- Provide a focal point for the resolution and/or discussion of information risk issues
- Ensure that the Executive Management Team are adequately briefed on information risk issues

4.2 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 has responsibility for ensuring that clinical information is appropriately managed and may be required to support the management and assessment of associated information risks.

4.3 Data Protection Officer

The Data Protection Officer (DPO) should 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 any way, 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 and be part of the approval process regarding Data Protection Impact Assessments (DPIA), and monitor performance
- Cooperate with the supervisory authority
- Be the contact point with the Information Commissioners Office for Information Governance breaches and incidents.
- Ensure that where an incident is likely to result in a risk to the rights and freedoms (as defined in UK GDPR) of Data Subjects that the ICO is informed no later than 72 hours after the organisation becomes aware of the incident.

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.

4.4 Information Asset Owners (IAOs)

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.

4.5 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 recognising actual and potential security incidents and consult the appropriate IAO on incident management, ensure their directorate's Information Asset Registers and Data Flow Mapping sheets are accurate and up to date and identify any actual or potential risks that need further consideration by the IAO/SIRO.

4.6 All Staff

All staff have a legal duty of confidentiality to keep personal information and commercially confidential information secure and private, and not to divulge information accidentally. Staff may be held personally liable for a breach of confidence and should ensure that:

- They comply with all policies, guidance and arrangements for using information appropriately and for keeping it secure.
- Undertaking all relevant training associated with role.
- Confidential information is kept secure and only accessed on a need–to-know basis
- Adhere to all the risk and incident reporting policies/procedures
- Bring to their line managers any concerns regarding information governance and risk

- They are aware of what could be classed as an information security incident or breach of confidentiality and know the process to follow and the forms to complete, so that incidents can be identified, reported, monitored and investigated.

5 Definitions/explanations of terms used

Information risk management is the process of understanding and responding to factors that may lead to a failure in the confidentiality, integrity or availability of an information system.

Information security risk is the potential or real harm that may be done to a system or process and its related information, whether intentionally or accidentally.

Risk

The chance (probability) of something happening which will impact in an adverse way something of value. This may be damage to information or reputation or may involve injury or liability. In this context risk is measured as a product of "consequence" x "likelihood" which are given numerical values as will be explained below.

Consequence

The result of a risk becoming a reality. For example, resulting in injury, financial loss or damage. There may be more than one consequence for each risk occurring.

Likelihood

What is the possibility of the risk occurring (becoming an issue).

Assessment

The process of identifying and evaluating risks.

Management

In this context, the management of the risk processes within an organisation.

Treatment

Ways of mitigating risk. General risks mitigation involves avoidance, reduction of the risk (consequence, likelihood, or both), transfer the risk to someone else, accept the risk.

6 Details of Process

The ICB has implemented a structured information risk assessment programme. This involves all information assets and flows being listed in the organisation's Information Asset Register (IAR) and Data Flow Maps (DFM). This ensures that the organisation understands what information is being held, where it is stored, how it is accessed and how it is shared. The IAR and DFM will be subject to an annual review and risk assessment.

All assets identified in the IAR as ‘business critical’ (i.e. fundamental to the delivery of the organisation’s business) will be subject to a more formal risk assessment and details of the mitigating controls documented and their effectiveness tested in relevant Business Continuity Plans (BCPs).

Risks to personal and special category data that arise as a consequence of changes to, or the introduction of new systems/process will be identified via the completion of a Data Protection Impact Assessment (DPIA) which identifies and mitigates information risks. DPIA’s are formally reviewed by the SCW IG Consultant and approved by SCW CSU Senior IG Consultant and the ICBs Deputy Senior Information Risk Owner and Data Protection Officer. Information Assets identified during this process will be included in the IAR and DFM documents.

6.1 IAO and IAA Work Programme

The SCW IG Team will support an annual work programme of related activities in order to produce a documented information risk report for the SIRO. IAOs will support the activities undertaken in the annual Work Programme and report back to the SCW Information Governance Team.

Alongside the work programme, the SCW Cyber Security Manager will ensure that an information security risk assessment and management process is in place to identify, implement and manage controls in place to reduce risk to the ICB’s systems and information assets managed by SCW.

6.2 Data Protection Impact Assessments (DPIA)

The General Data Protection Regulation introduced an obligation to complete a DPIA before carrying out types of processing likely to result in high risk to individuals’ interests. This is a key element of the new focus on accountability and data protection by design. DPIAs are now mandatory in some cases, and there are specific legal requirements for content and process.

A DPIA is a way to systematically and comprehensively analyse processing activities and help identify and minimise data protection risks. DPIAs should consider compliance risks, but also broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm - to individuals or to society at large, whether it is physical, material or non-material.

To assess the level of risk, a DPIA must consider both the likelihood and the severity of any impact on individuals. A DPIA does not have to eradicate the risks altogether but should help to minimise risks and assess whether or not remaining risks are justified.

DPIAs are a legal requirement for processing that is likely to be high risk. But an effective DPIA can also bring broader compliance, financial and reputational benefits, helping demonstrate accountability and building trust and engagement with individuals.

A DPIA may cover a single processing operation or a group of similar processing operations. A group of controllers can do a joint DPIA.

It’s important to embed DPIAs into organisational processes and ensure the outcome can influence plans. A DPIA is not a one-off exercise and should be seen as an ongoing process, and regularly review it.

The ICB has a comprehensive template and guidance document that form part of the DPIA framework and a route for approval. All completed DPIAs should be sent to the SCW Information Governance Team.

6.3 Information Risk Management Process

All information risks will be recorded, managed and escalated in accordance with the ICB Risk Management Policy and Procedure and the Standard Operating Procedure for managing Information Risk Incidents (see Appendix).

Any incidents will be graded by the SCW IG Consultant according to the significance of the breach and the likelihood of the consequences occurring. The incident is graded according to the impact to the individual or group of individuals. NHS England national guidance detailed in Standard Operating Procedure for managing Information Risk Incidents. The DPO and Deputy DPO will have access to the ICB incident reporting system to allow audit of incidents. IGG will be provided with a quarterly report so there is oversight of all incidents to ensure approval of grading.

Any incident graded 6 and above will be reported to the DPO. The SIRO/CG and DPO will decide whether an incident is externally reportable.

Risks will be managed as follows:

A – Local level management.

The risk will be identified as part of team/Directorate risk register or asset register.

B – SIRO managed.

The risk will be listed as part of the SIRO IG risk register (Finance register).

C – Executive Management Team oversight.

All risk are reported to the ICBs Information Governance Group. High Risks will be included in the directorate risk register which feed the Corporate Risk Register.

7 Training requirements

All staff will undertake Information Governance training called Data Security Awareness via the Consult OD link or where appropriate and agreed via face to face training sessions. Extra training will be given to those who need it such as IAOs/IAAs and those dealing with requests for information. Support is available from the CSU IG team.

ICB staff are also mandated to download and read the Data Security and Information Governance staff handbook and the ICBs Acceptable Use Policy.

There is an extensive guidance document that accompanies the DPIA template that enables staff to understand the types of information risk that can occur and encourage them to embed a ‘privacy by design and default’ approach at the beginning of new projects and activities.

8 Equality Impact Assessment

EIA screening has been completed and reference as an appendix.

9 Implementation and Monitoring Compliance and Effectiveness

The following actions are implemented to ensure there is a regular review of information risk; these activities are all under the oversight of the Information Governance Group:

- Monitoring of information security and risk processes through the ICB’s Data Security and Protection Toolkit Submission. This is overseen by the SIRO.
- Regular review and audit of information flows to ensure confidential information is being transferred securely and in order to reduce information risk. This is co-ordinated by SWC CSU Information Governance Consultant and completed by Information Asset Owners.
- Implementation of actions plans or internal or external auditor reports
- Analysis of information incidents will support the ICB in understanding the real level of risk being experienced and in adjusting the controls in place

10 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.

11 References, acknowledgements and associated documents

- ICB Information Governance Framework and Strategy
- ICB Information Governance Policy
- ICB Confidentiality and Security of Information Policy
- SCW IT Policies
- ICB DPIA Framework and Guidance
- ICB Incident Reporting Process
- Standard Operating Procedures for Information Risk Incidents

12 Appendices

12.1 Standard Operating Procedures

Standard
Operating Procedur

12.2 Equality Impact Assessment

EHIA for IG Risk
Management proce:

12.3 Implementation Plan

Target Group	Implementation or Training objective	Method	Lead	Target start date	Target End date	Resources Required
Staff	Awareness of Policy	Re-launch of Policy at HWGNFY, The Voice	AG/Comms	Oct 24	Oct 24	
Staff	Access to policy	Upload on to Hub	Comms	Oct 24	Oct 24	
IAO/IAA	Access to Policy	Distribution	AG	Oct 24	Oct 24	