NHS
Bedfordshire, Luton and Milton Keynes
Integrated Care Board

Information Governance Framework

Document Status:

This is a controlled document. Any printed or downloaded copies are not controlled. The version of this document published on the Bedfordshire, Luton & Milton Keynes Integrated Care Board website is the controlled copy www.befordshirelutonandmiltonkeynes.icb.nhs.uk

Sustainable Development - Environmental

Do you really need to print this document?

Please consider the environment before you print this document and where possible copies should be printed double-sided. Please also consider setting the page range in the print properties, when relevant to do so, to avoid printing the document in its entirety.

Document Control	
Document Owner:	Senior Information Risk Owner
Document Author(s):	Head of Safe Practice & DPO
Directorate:	Medical Directorate
Approved By:	The Board of the Integrated Care Board
Date of Approval:	20-01-2025
Date of Next Review:	20-01-2027
Effective Date:	01-07-2022

Version Control			
Version	**Date**	**Reviewer(s)**	**Revision Description**
v1.0	01-07-2022		The Board of the Integrated Care Board adopted the policy as approved.
Draft V2.0	4-12-2024	Head of Safe Practice & DPO	Removal of IG Strategy, as no longer required. Updated with further information relating to the DSPT and legal obligations.
Final V2.0	20-01-2025	Operational Group	The Operational Group approved the minor changes due to the biennial review.

Implementation Plan

Development and Consultation:	The following individuals were consulted and involved in the development of this document: ▪ Information Governance Team (IGT) ▪ Information Governance Group (IGG) ▪ Data Protection Officer (DPO)
Dissemination:	Staff can access this document via the website and will be notified of new / revised versions via the staff briefing. This document will be included in the organisation's Publication Scheme in compliance with the Freedom of Information Act 2000.
Training:	The following training will be provided to make sure compliance with this document is understood: All new staff are required to attend a compulsory Induction Programme which incorporates Information Governance.

	In addition to this, all staff are required to annually complete and pass the NHS Digital's Data Security Awareness Level 1 module on the Electronic Staff Record (ESR) e-Learning portal. Please also refer to the Training Needs Analysis (TNA) section of this policy.
Monitoring:	Monitoring and compliance of this document will be carried out via: The Information Governance Group with progress reported to the Audit and Risk Assurance Committee. An assessment of compliance with assertions which make up the Data Security and Protection Toolkit, will be undertaken each year and audited by internal auditors. In addition, the ICBs Information Governance Department will undertake additional monitoring of compliance with this policy as a response to identification of any gaps or as a result of risks identified by incidents, external reviews or other sources of information and advice
Review:	The Document Owner will ensure this document is reviewed in accordance with the review date on page 2.
Equality, Diversity and Privacy:	Appendix 1 - Equality Impact Assessment Appendix 2 - Data Protection Impact Assessment
Associated Documents:	The following documents must be read in conjunction with this document: o Data Protection Policy o Information Sharing Policy o Asset Management Policy o Subject Access & Access to Health Records Policy o Records Management & Lifecycle Policy o Social Media Policy o Integrated Risk Management Policy o Offsite Storage Procedures o Controlled Environment for Finance Procedures o Information & Cyber Security Incident Procedure o Working From Home Guidance o Staff IG Handbook
References:	The following articles were accessed and used to inform the development of this document: o Records Management Code of Practice for Health and Social Care (2021) o Caldicott Principles o A Manual for Caldicott Guardians (2017) o Information: To Share or Not to Share (2013) (Caldicott2) o Review of Data Security, Consent and Opt-outs (2016) (Caldicott 3) o General Data Protection Regulation (UKGDPR) o Data Protection Act 2018 o NHS Code of Practice for Confidentiality and Trust's Secure Data Handling Policy

Table of Contents

1.0 Introduction

1.1 NHS Bedfordshire, Luton and Milton Keynes Integrated Care Board (ICB) aims to ensure robust governance through its formal written procedural documents, such as this document, which communicate standard organisational ways of working. These documents help clarify operational requirements and consistency within day-to-day practice. They can improve the quality of work, increase the successful achievement of objectives and support patient safety, quality and experience. The ICB aims to ensure its procedural documents are user friendly, up-to-date and easily accessible.

1.2 The ICB must design and implement procedural documents that meet the diverse needs of our service and workforce, ensuring that none is placed at a disadvantage over others, in accordance with the Equality Act 2010. The Equality Impact Assessment initial screening, which was used to determine the potential impact this policy might have with respect to the individual protected characteristics is incorporated at Appendix 1 - Equality Impact Assessment Initial Screening.

1.3 The Information Governance Framework is setup in line with the direction and boundaries of the ICB Data Protection Policy. To ensure compliance a Data Protection Impact Assessment is a process which helps assess privacy risks to individuals in the collection, use and disclosure of personal information. The Data Protection Impact Assessment initial screening, which was used to determine the potential impact this policy might have with respect to an individual's privacy is incorporated at Appendix 2 - Data Protection Impact Assessment Initial Screening.

1.4 Information Governance is the term used to describe the arrangements put in place by NHS organisations to ensure that information (data) is handled in a confidential and secure manner to appropriate legal, ethical, and quality standards.

2.0 Scope

2.1 The scope of this policy, includes, but is not limited to the following areas:

- Information Governance Management
- Confidentiality and Data Protection Management
- Information security and supports cyber management security
- Data Sharing
- Pseudonymisation and Anonymisation
- Records Management
- Incident Reporting
- Freedom of Information
- Risk Management

2.2 This policy applies, to all ICB staff members, including Ordinary Members of the Board of the ICB, and Practice Representatives, involved in the ICB's policy,

making processes, whether permanent, temporary or contracted-in under a contract for service (either as an individual or through a third-party supplier), here in after referred to as 'staff'. Furthermore, the policy applies to all vendors, service companies, partners and third parties that are processing ICB data.

2.3 Failure to adhere to this policy may result in disciplinary action and/or referral to the regulatory body to which a staff member may be registered. Furthermore, it may result in terminating contract with vendors, service companies, partners and third parties that are processing ICB data.

2.4 This Policy covers all aspects of information within the ICB, including but not limited to, patient/client/service user information, staff information etc. held in any format e.g., paper, electronic etc.

3.0 Definitions

This section provides all readers with an explanation of terms used within this policy.

3.1 Concept of Confidentiality

3.1.1 A duty of confidentiality arises when a person or organisation discloses information to another person or organisation under conditions where it is realistic to expect that the information provided will be treated in confidence.

3.1.2 Disclosure of this information can either be authorised or unauthorised where only limited staff members have the authority to disclose information.

3.1.3 A breach of confidentiality is the unauthorised disclosure of information provided in confidence.

3.2 Confidential Information

3.2.1 Confidential information can be anything that relates to patients, staff or any other sensitive information (such as contracts and tenders, classified documents) held in any form (such as paper, electronic, microfilm, audio or video) howsoever stored (such as patient records, paper diaries, computer or on mobile devices such as laptops, tablets, smartphones) or even passed by word of mouth.

3.3 Data Controller

3.3.1 A data controller means a person, organisation or public authority who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

3.4 Data Processor

3.4.1 A data processor, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

3.5 Personal Data

3.5.1 This means data which relate to a living individual who can be identified from those data and includes any expression of opinion about the individual. Typical examples of this type of data could include;

- Person's name, address, full postcode, date of birth.
- Email address and telephone numbers.
- Pictures, photographs, videos, audiotapes or other images of patients.
- NHS number or local unique identifiers, these are considered identifiable if the organisation holds the means to re-identify the person from this unique identifier.
- Any other data, or linked data, that may be used to identify a patient directly or indirectly. For example, rare diseases, drug treatments or statistical analyses which have very small numbers within a small population may allow individuals to be identified.

3.6 Special Category Data

3.6.1 Data held about an individual which contains both personal and sensitive information. Under the UKGDPR the following types of information are deemed as special category:

- Race,
- Ethnic origin,
- Religious or other beliefs,
- Political opinions,
- Trade union membership,
- Genetics,
- Biometrics (where used for ID purposes),
- Physical or mental health,
- Sexual life, and
- Criminal proceedings or convictions.

3.7 Processing

3.7.1 Processing means obtaining, recording, holding the information or data or carrying out an operation on the information or data. An operation could include organising, adapting or altering the data. It also includes retrieving, consulting, linking to other data sources or using the information or data.

3.7.2 Disclosing the information or data by transmission or dissemination indicates processing as does alignment, combination, blocking, erasure, and destruction.

Viewing data on a computer screen is considered to be processing under the Data Protection Act 2018 and the UKGDPR.

3.8 Information Commissioner's Office (ICO)

The ICO is our regulator and issues guidance, help and support. They can also investigate us regarding complaints and incidents and can issue penalties.

Further information relating to the ICO can be below or via Information Commissioner's Office (ICO).

4.0 Policy Statement

The purpose of this framework is to enable all staff to understand their obligations regarding any information which they come into contact in the course of their work and to provide assurance that such information is dealt with legally, securely, fairly and in line with current Data Protection Legislation.

The ICB will ensure that:

- There is an adequate Information Governance Framework to support the current and evolving Information Governance agenda at local, regional and at a national level e.g. ICS IG priorities, National Data Opt-out Programme.
- There are approved, consistent and comprehensive Information Governance related Policies, Standard Operating Procedures with associated strategies and/or improvement plans that are in line with the overall ICB Digital Strategy and the overarching ICS Information Governance and Data Security priorities.
- That the flow of data in the organisation is identified including the data controllers and processors.
- That the legal basis for processing data for every function is identified and understood including ensuring the transparency about purpose and process, supporting good practice, and promoting public engagement.
- Any patient and service user information rights are considered.
- Adherence to current published guidance on cyber security for health and care.
- Formal contractual arrangements that include compliance with Information Governance and GDPR are in place with all contractors and support organisations.
- Employment contracts which include compliance with information governance standards are in place for all individuals carrying out work on behalf of the ICB.
- Information Governance awareness and mandatory training procedures are in place and all staff are appropriately trained.
- Consider and action any IG risks raised through the appropriate governance structure.

4.1 What is Information Governance?

IG ensures necessary safeguards for, and appropriate use of, patient and staff personal information. Key areas include:

- Confidentiality: The ICB follows the NHS Code of Practice for Confidentiality available at: https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-informationgovernance/codes-of-practice-for-handling-information-in-health-and-care/code-of-practice-onconfidential-information
- Data Security and Protection Toolkit (DSPT): an annual self-assessment related to information and cyber security and IG. Further information within section 6.
- Data Security: The DSPT is required to provide technical assurance of the safeguards protecting patient and staff data, through clear guidelines and cyber security counter measures. We have adopted our IT providers (HBLICT) Information Security Policy as our own as we have a managed service.
- Looking after health and care information: Protecting personal confidential data is central to all that we do, so we treat it with the greatest of care and respect. The Trust's Secure Data Handling Policy is available on the Trust's Intranet. National guidance is available at: https://digital.nhs.uk/dataand-information/looking-after-information
- NHS Codes of Practice and Legal obligations: for confidentiality, information security management and the Records Management NHS Code of Practice are available at: https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-informationgovernance/codes-of-practice-for-handling-information-in-health-and-care/records-management-codeof-practice-for-health-and-social-care-2016

There are several legal obligations placed upon the ICB for the processing of personal identifiable information which it MUST comply with. The key ones are:

- Data Protection Act 2018
- UK General Data Protection Regulations (UKGDPR)
- Access to Health Records (Deceased) Act 1990
- Common Law Duty of Confidentiality
- Human Rights Act 1998
- Computer Misuse Act 1990
- Health and Social Care Act 2012
- Health and Social Care (Safety and Quality) Act 2015
- Health and Care Act 2022
- Privacy and Electronic Communications Regulations

The UKGDPR is the key legislation and sets out clear obligations for the ICB and rights for data subjects. The key obligations are listed below in section 6 of this policy. Rights of the data subjects are also detailed in section 6.

4.2 Accountability

Accountability is one of the key UK GDPR data protection principles. It requires the ICB to put appropriate technical and organisational measures in place to meet the requirements of UK GDPR and be able to demonstrate compliance. This framework supports our accountability obligations.

The ICB has several measures in place including, but not limited to:

- IG, IT Security and Cyber Security policies, including policies for the effective and secure management of its information assets and resources.
- IG & data protection procedures and staff guidance – see IG section on the ICBs Staff Intranet.
- A privacy by design and default approach – see Data Protection Policy.
- Written contracts in place with organisations that process personal data on the ICBs behalf.
- A record of the ICBs processing activities, including the legal basis for each activity.
- Recording, investigating, learning from and where necessary, reporting personal data breaches.
- An appropriately trained and supported DPO.
- Mandatory Data Security & Protection staff training – see section 6.
- Fair Processing Notices – see Data Protection Policy.
- Regular assessments and audits of the ICBs information and IT security arrangements as part of the annual review and submission of the DSPT.
- Promoting effective cyber and information security practice to staff through policies, procedures, training and communication of alerts.
- Records Management and Information Lifecycle Policy and guidance covering all aspects of records management, consistent with the Records Management Code of Practice for Health and Social Care 2016 – see Record Management and Information Lifecycle Policy and Guidance.
- Promote data quality through policies.

There are also several NHS standards which the ICB must comply with, including, but not limited to:

- Records Management Code of Practice for Health and Social Care (2021)
- Caldicott Principles
- A Manual for Caldicott Guardians (2017)
- Information: To Share or Not to Share (2013) (Caldicott2)
- Review of Data Security, Consent and Opt-Outs (2016) (Caldicott 3)

The ICB will perform an annual assessment of its compliance against the assertions which make up the DSPT and have the evidence provided for the assessment further assessed by its internal auditors.

The ICB will conduct periodic reviews and audits to ensure the way it manages its records is in line with statutory obligations and NHS standards.

5.0 Roles and Responsibilities

The following roles and responsibilities are in place to implement, govern and manage Information Governance / data protection and confidentiality.

5.1 The Board of the Integrated Care Board

The Board is accountable for the effectiveness of the Information Governance

Framework, the compliance to the relevant internal and external laws and regulations as part of the internal control system and for ensuring that the necessary support and resources are available for the effective implementation of the Data Protection Policy and this Information Governance Framework. It has responsibility for the IG agenda supported by identified senior roles which they are required to appoint including the Caldicott Guardian, Senior information Risk Owner and Data Protection Officer.

5.2 Audit and Risk Assurance Committee

The Audit and Risk Assurance Committee will receive regular IG Reports via the IG Group. The Senior Information Risk Owner is a regular attendee at the Audit and Risk Assurance Committee. The ARAC will also receive the Internal Auditors independent review of the DSPT assessment.

The committee on behalf of the Integrated Care Board, will have oversight on the assurance for the information governance framework.

5.3 Information Governance (IG) Group

- The Information Governance (IG) Group (the Group) is established to support the Chief Financial Officer in their capacity as Senior Information Risk Officer (SIRO).
- The Chair of the IG Group is the Senior Information Risk Owner. Other members of the group include the Caldicott Guardian, and the Head of Safe Practice/Data Protection Officer.
- The Group will approve the operational arrangements for ensuring appropriate safekeeping and confidentiality of records and for the storage, management and transfer of information and data. In addition, the Group will:
    - coordinate, supervise and direct the work of others as appropriate to ensure the ICB maintains a co-ordinated approach to IG.
    - will provide regular reports to the Audit and Risk Assurance Committee and Finance and Investment Committee as required
    - also sign off final submission of the Data Security & Protection Toolkit (see section 6 below) with advice from the Head of Safe Practice & Data Protection Officer (see section 5.6 below).

5.4 Senior Information Risk Owner (SIRO)

The SIRO has overall responsibility for the implementation of risk management across the ICB, for ongoing management of information risks and is the owner of the ICB's Information Asset Registers and Information Risk Registers.

The SIRO is a member of the Board and provides advice to the Chief Executive Officer on the content of the Annual Governance Statement and the Statement of Internal Control in regard to information risk.

The SIRO is supported by Information Asset Owners, the ICB's Caldicott Guardian, the Head of Digital Delivery and the Head of Safe Practice/Data Protection Officer.

Key responsibilities:

- To own the ICB's overall information risk assessment process and for ensuring information asset risk reviews are completed.
- Oversee the development of an Information Risk Policy, and a strategy for implementing the policy within the existing Information Governance Framework.
- For ensuring that all information risks are recorded, controls have been identified and mitigated where applicable including, but not limited to, ensuring that all records management issues (including electronic media) are managed in accordance with this Framework.
- To oversee the development of an information governance framework and the integrated privacy management system.
- Establish and chair BLMK ICB IG Group, whereby Information Governance and Data Protection can be discussed and escalated to Board.
- To take ownership of the risk assessment process for information and cyber security risk, including review of the annual information risk assessment to support and inform the Statement of Internal Control.
- Review and agree action in respect of identified information risks.
- To ensure that the ICB's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff.
- To provide a focal point for the resolution and/or discussion of information risk issues.
- To ensure the Board is adequately briefed on information risk issues.
- To advise the Chief Executive Officer and the Board on Data Protection with support from the Caldicott Guardian (CG) and Data Protection Officer (DPO), and information risk management strategies and provide periodic reports and briefings on progress.
- Ensure that all care systems information assets have an assigned Information Asset Owner.

5.5 Caldicott Guardian (CG)

The Caldicott Guardian has a strategic and advisory role with particular focus on ensuring patient identifiable information is shared in an appropriate and secure manner. They are known to be the conscience of the organisation, as they will look at a situation from the perspective of a patient/service user. They are supported in their role by the IG Group.

Key responsibilities:

- Strategy and Governance - which involves representing and championing confidentiality and information sharing requirements and issues at senior management level and, where appropriate, at a range of levels within the organisation's overall governance framework e.g. Board/executive management team level and sits on the ICBs IG Group.
- Confidentiality and Data Protection expertise - develops a strong knowledge of confidentiality and data protection matters, drawing upon support from internal and external sources of advice and guidance where available and applicable.
- Internal information processing - ensures that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff.

- Information sharing - oversees arrangements, protocols and procedures where confidential personal information is shared with external bodies including social care and safeguarding. This includes flows of information to and from partner agencies, sharing through IT systems, disclosure for research and disclosure to the police and other enforcement authorities.
- Subjects Rights – provide approval for the release of information requested under the data subject's right of access (known as subject assess requests (SAR) and the Access to Health Records (deceased) Act.

5.6 Head of Safe Practice & Data Protection Officer (DPO) (IG Lead)

The Head of Safe Practice will drive the strategic development of information governance and integrated privacy management for the ICB and the partners of the ICS and will be responsible for developing and implementing a fit for purpose information governance framework that takes account of best practice from national policy.

The IG lead is accountable for ensuring effective management, accountability, compliance, and assurance for all aspects of IG. The key tasks of an IG Lead include:

- developing and maintaining the currency of comprehensive and appropriate documentation that demonstrates commitment to and ownership of IG responsibilities, e.g. an overarching high-level strategy document supported by corporate and/or directorate policies and procedures;
- ensuring that there is top level awareness and support for IG resourcing and implementation of improvements;
- providing direction in formulating, establishing and promoting IG policies;
- establishing working groups, if necessary, to co-ordinate the activities of staff given IG responsibilities and progress initiatives;
- ensuring annual assessments using the DSPT and audits of DSPT policies and arrangements are carried out, documented and reported, in line with the requirements of the NHS Standard Contract;
- ensuring that the annual assessment and improvement plans are prepared for approval by the senior level of management, e.g. the board or senior management team, in a timely manner.
- ensuring that the approach to information handling is communicated to all staff and made available to the public;
- ensuring that information governance staff understand the need to support the safe sharing of personal confidential data for direct care, as well as the need to protect individuals' confidentiality;
- ensuring that appropriate training is made available to all staff and completed as necessary to support their duties.
- liaising with other committees, working groups and programme boards in order to promote and integrate IG standards;
- monitoring information handling activities to ensure compliance with law and guidance;
- providing a focal point for the resolution and/or discussion of IG issues.

The DPO is actively supporting management in its responsibility for monitoring compliance with data protection law and ensuring data practices comply with applicable legislation and guidance. The DPO is the primary contact for data subjects (individuals

whose data is processed by the ICB) and the Information Commissioners Office (ICO – the body which enforces Information Rights laws and regulations), with whom they are registered.

.

The DPO reports to the SIRO on relevant matters who will escalate any serious concerns or issues to the Board.

The DPO is a legally required role as part of the UKGDPR accountability principle, which is one of the key principles for data protection. Their job description must be compliant with UKGDPR requirements, and they must have:

- Direct access to the highest management level of the organisation – this does not necessarily imply line management at this level, but direct and unimpeded access to the senior management team.
- Adequate resources (sufficient time, financial, infrastructure, and, where appropriate, staff) to enable the DPO to meet their UK GDPR obligations, and to maintain their expert level of knowledge Proven 'expert knowledge of data protection law and practices', the ability to perform the tasks specified in the UKGDPR, and sufficient understanding of the organisation's business and processing.
- Timely involvement in all data protection issues.
- Involvement in incident management.
- Timely access to all relevant information on the DPO's request.
- Have their contact details published in transparency information for subjects and communicated to the ICO through the DPO registration process.

In addition, the DPO must operate independently and is not dismissed or penalised for performing their statutory duties and where the DPO performs another role or roles, there must be no conflict of interest between the various roles.

5.7 Information Asset Owners (IAOs)

5.7.1 IAOs are directly accountable to the SIRO and must provide assurance that information risk is being managed effectively in respect of the information assets that they are owners of.

5.7.2 IAOs also lead and help foster, within their respective Directorates, a culture that values, protects and uses information.

5.7.3 IAOs are generally at director level (so senior enough to make decisions concerning their assets), although they can delegate this role to a responsible deputy.

5.7.4 Their role is also to understand and assess risks to their information asset and to provide assurance to the SIRO on the security and use of those assets. They ensure that all threats, vulnerabilities, and impacts are properly assessed and included in their Information Asset Register (IAR).

5.7.5 IAOs can assign day to day responsibility for each information asset to an administrator or manager known as an Information Asset Administrator (see section 5.8 below).

5.7.6 The SIRO is responsible for the appointment and management (in terms of information assets) of the IAOs. IAOs are expected to understand the overall business goals of the organisation and how the information assets they own contribute to and affect these goals.

5.7.7 IAO's will take appropriate actions to:

- Know what information the asset holds and understands the nature and justification of any information flows to and from the asset.
- Know who has access to their assets and why, and ensure their use is monitored and compliant with policy.
- Ensure the confidentiality, integrity, availability, and authenticity of all information that their system creates, receives, maintains, or transmits and protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
- Conduct Data Protection Impact Assessments in line with the ICB's Data Protection Policy.
- Participate in the ICBs Information Asset Register review process by ensuring their IARs are kept up to date and are accurate.
- Appoint Information Asset Administrators, where appropriate.
- Understand and address risks to the asset, report in line with the ICBs Risk Management Policy and provide assurance to the SIRO.

Further information related to Information Asset Management can be found within the ICB Asset Management Policy.

5.8 Information Asset Administrators (IAAs)

5.8.1 IAOs are responsible for appointing Information Asset Administrators (IAAs). It is at the IAOs discretion how many IAAs are appointed to support them in their role.

5.8.2 IAAs are operational staff with day-to-day responsibility for managing risks to their information assets.

5.8.3 Responsibilities of the IAA:

- Providing support to their IAOs to ensure that policies and procedures are followed and to recognise potential or actual security incidents.
- Consulting their IAOs on incident management to ensure that information asset registers are accurate and maintained up to date.
- Ensuring compliance with relevant Information Sharing Agreements (ISAs) and that information handling procedures are fit for purpose and are properly applied.
- Under the direction of their IAO, they will ensure that personal information is not unlawfully processed, and they will, upon recognising new information

handling requirements (e.g. a new type of information arises) that the relevant IAO is consulted over appropriate procedures.

- They will consult with the IAOs regarding any potential or actual security incidents.
- Reporting to the relevant IAO on current state of local information handling and ensure that local information handling constraints (e.g. limits on who can have access to the assets) are applied, referring any difficulties to the relevant IAO.
- They will act as first port of call for local managers and staff seeking advice on the handling of information.
- Under the direction of their IAO, they will ensure that information is securely destroyed when there is no further requirement for it.

5.9 Heads of Departments/Services

5.9.1 All Head of Departments/Services within the ICB are responsible for ensuring that their staff are aware of and comply with the ICBs IG policies and supporting standards and guidelines and for ensuring they are built into departmental processes and procedures.

5.10 All Staff

5.10.1 IG compliance is a legal and contractual obligation for all staff.

5.10.2 Staff should note that there are confidentiality clauses in their contract and that they are required to participate in induction, annual mandatory training and comply with the ICBs IG policies and supporting guidelines.

5.10.3 Any breach of confidentiality, inappropriate use of information or abuse of computer systems is a disciplinary offence, which may result in dismissal or termination of contract.

5.10.4 All employees are personally responsible for compliance with the law in relation to the UK General Data Protection Regulation, Data Protection Act 2018, and the Common Law Duty of Confidentiality.

5.11 Contracted Third Parties

5.11.1 It is not unusual to have third parties gaining access to the ICB's information assets and for them to process personal identifiable information on behalf of the ICB. These third parties have appropriate information governance clauses included in their contracts and where appropriate, the contract is underpinned with a Data Processing Agreement.

5.11.2 Third parties which have been through the procurement process are required to demonstrate their compliance with IG by annually completing and submitting a DSPT and registering with the ICO as well as complying with a number of

information security questions within the Data Protection Impact Assessment and during the procurement process.

Those third-party suppliers which have not been through the procurement process, will also be required to provided sufficient assurance in relation to information security.

5.11.3 A register of all contracts is maintained by the ICBs Contracts Department and information related to information assets is held within the information asset register.

5.12 Information Commissioners Office

As stated within section 3.8 above**,** the ICO is our regulator and issues guidance, help and support to both organisations processing personal data and the data subjects (e.g. members of the public, patients, staff etc). They can also investigate us regarding complaints and incidents and can issue penalties.

- **Payment of a Fee to the ICO**

The ICB must pay a fee to the ICO, on an annual basis, and will have their details published by the ICO in a Data Protection Register.

The ICOs Data Protection Register can be viewed here https://ico.org.uk/about-the-ico/what-we-do/register-of-fee-payers/

- **Reporting Breaches to the ICO**

The ICB must report certain personal data breaches to the ICO within 72 hours of becoming aware of the breach, where feasible.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms (see Rights of the Data Subject in section 6), the ICB must also inform those individuals without undue delay.

For breach reporting procedures please see section 6.

- **Monetary Penalty Notice (for serious non-compliance)**

The Criminal Justice and Immigration Act 2008 extends the powers of the Information Commissioner under DPA18 to allow fines of up to £500,000 for individuals or organisations found guilty of deliberate or reckless disclosure of information, including failure to take appropriate security precautions.

In addition, individuals can receive a prison sentence on conviction of an offence under DPA and fines for organisations from the ICO under UKGDPR can be up to £17.5 million.

6.0 Processes and Procedures

6.1 Data Security and Protection Toolkit

6.1.1 The ICB is mandated to use the Data Security & Protection Toolkit (DSPT) to measure its compliance with IG. The ICB is required to submit a DSPT assessment each year following internal audit review of the evidence provided.

6.1.2 The ICB's performance against the assertions which make up the DSPT are reported to the Department of Health and forms a part of the assurance processes associated with the Care Quality Commission; NHS England (NHSE)) and the NHS Resolution risk management standards.

6.1.3 The outcome of the ICB's annual Data Security and Protection Toolkit Assessment is reported to the IG Group and the Audit and Risk Assurance Committee.

6.1.4 Since September 2024, the ICB (as a category 1 organisation) is self-assessing against the National Cyber Security Centre's Cyber Assessment Framework (CAF) as its basis for cyber security and IG assurance. We will self-assess our level of compliance against each outcome using the indicators of good practice as a guide as instructed by NHS England.

6.1.5 HBLICT as the ICBs IT provider is responsible for ensuring the ICBs Head of Safe Practice/DPO is provided with the information and documentation necessary for the ICB to be able to evidence compliance with IT Security & Cyber Security outcomes.

6.2 Caldicott Principles

6.2.1 The Caldicott Committee Report on the Review of Patient-Identifiable Information 1997 found that compliance with confidentiality and security arrangements was patchy across the NHS and identified six good practice principles for the health service when handling patient information. These principles can be extended to also apply to social care service user information.

6.2.2 A further review was published in March 2013 which amended the Caldicott Principles, as follows:

- Justify the purpose(s)
- Don't use personal confidential data unless it is absolutely necessary
- Use the minimum necessary personal confidential data
- Access to personal confidential data should be on a strict need-to-know basis
- Everyone with access to personal confidential data should be aware of their responsibilities
- Understand and comply with the law

- The duty to share information can be as important as the duty to protect patient confidentiality.

6.2.3 Further details about the revised Caldicott Principles and how to apply them can be found in the Data Protection Policy.

6.3 Freedom of Information (FOI) Act 2000

6.3.1 Information about the organisation will be available to the public in line with the Freedom of Information Act, Environmental Information Regulations and Protection of Freedoms Act unless an exemption applies. The ICB maintains a Publication Scheme in line with legislation and guidance from the Information Commissioner – see Freedom of Information Policy.

6.4 Legal obligations

There are several legal obligations placed upon the ICB for the processing of personal identifiable information, the key ones are:

Common Law Duty of Confidentiality

Common law duty of confidentiality is not a written law, it is common law based on legal precedent from historical legal cases.

The common law duty of confidentiality means that information confided by a Patient / service user or otherwise obtained (e.g. during medical examination or when receiving personal care), where it is expected that a duty of confidence applies, should not generally be used, or disclosed further, except as originally understood by the confider or with their subsequent permission.

This duty of confidentiality may be set aside, and confidential information disclosed where it is in the public interest or when it is a legal requirement to do so – see Information Sharing Policy

Human Rights Act

Article 8 of the Human Rights Act establishes the right to respect for an individual's private and family life. Compliance with the Data Protection Act 2018 and the common law duty of confidentiality will satisfy this right.

UK General Data Protection Regulations & Data Protection Act 2018

The Data Protection Act 2018 (DPA18) sets out the framework for data protection law in the UK. It updates and replaces the Data Protection Act 1998 and came into effect on 25 May 2018. It was amended on 01 January 2021 by regulations under the European Union (Withdrawal) Act 2018, to reflect the UK's status outside the EU.

DPA18 sits alongside and supplements the UK General Data Protection Regulations (UK GDPR) by providing exemptions and sets the Information Commissioner's functions and powers.

The Information Commissioners Office is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. They regulate data protection compliance in the UK promote good practice, monitor breach reports, conduct audits and advisory visits, consider complaints, monitor compliance and take enforcement action where appropriate.

The UK General Data Protection Regulation (UK GDPR) is a UK law which came into effect on 01 January 2021. It sets out the key principles, rights and obligations for most processing of personal data in the UK, except for law enforcement and intelligence agencies.

It is based on the EU GDPR (General Data Protection Regulation (EU) 2016/679 which applied in the UK until 31st December 2020, with some changes to make it work more effectively in a UK context.

Data protection laws take a flexible, risk-based approach, which puts the onus on the ICB to think about and justify how and why it uses personal data. It applies to all person identifiable information about living individuals held in any format, including, but not limited to paper documents, computer databases, visual images, audio recordings, CCTV footage, videos, emails etc. It also partly applies to deceased medical records.

Article 5 of the UK GDPR sets out 7 'Key Principles' (known as the Data Protection Principles) which lay at the heart of data protection law. Compliance with these principles is therefore a fundamental building block for good data protection practice and key to compliance with data protection law.

These principles stipulate that personal data must be:

- Processed fairly, transparently and lawfully processed
- Processed for limited and specific purposes
- Adequate, relevant and not excessive (i.e. minimised)
- Accurate and up to date
- Not kept longer than necessary
- Securely held with integrity and confidentiality
- Accountability

Further details about these principles and how to apply them can be found in the Data Protection Policy. For details about the 'Accountability' principle, please see section 4.

UK GDPR also sets out rights for data subjects. These are:

- The right of access
- The right to be informed
- Right to rectification
- Right to be forgotten
- Right to restriction
- The right to object to processing
- Automated decision making including profiling
- Portability

Further details about these rights, how to recognise a request from a data subject asserting one of their rights and details of how these are processed by the ICB, please see Subject access & Access to Health Records Policy and Data Protection Policy.

6.5 Incident Reporting

6.5.1 IG and IT related incidents, including cyber security incidents, must be reported and managed through the ICB's IG & Cyber Incident Reporting Procedure which requires the IG Team to be informed immediately of all IG, information security and cyber security incidents. These include, but are not limited to, NHS England's (NHSE's) classifications:

- Lost in transit
- Lost or stolen hardware
- Lost or stolen paperwork
- Disclosed in error
- Uploaded to website in error
- Non-secure disposal – hardware
- Non-secure disposal – paperwork
- Technical security failing (including hacking)
- Unauthorised access / disclosure

6.5.2 On receiving notification of a potential serious incident requiring investigation, the IG Team will inform the SIRO and Caldicott Guardian as soon as practicably possible (if they are not already aware) to seek advice and guidance, as appropriate.

6.5.3 All IG and IT related incidents will be reviewed by the IG team and where necessary escalated to NHSE , Department of Health and Social Care and the Information Commissioner's Office using the Incident Reporting functionalities of the DSPT.

6.5.4 The decision to report externally to the ICO is made in line with NHSE's Guide to the Notification of Data Security and Protection Incidents, with the ultimate decision being made by the SIRO, based on the advice of the DPO.

6.5.5 The DPO monitors IG incidents to identify trends and guide overarching remedial action to those trends.

6.6 Information Asset Management and Business Continuity

6.6.1 A core IG objective is that Information Assets (IAs) and the use of information held within them is identified and that the business importance/purpose is established.

6.6.2 IAs are those that are central to the efficient running of the ICB and specific departments, for example, clinical systems (such as Broadcare), record repositories (such as Datix) and so on. They also include, but are not limited to the following examples:

- Information – system documentation and procedures, archive media and data.

- Software – databases, application programs, systems, development tools and utilities.
- Physical – infrastructure, equipment, furniture and accommodation used for data processing.
- Services – computing and communications, heating, lighting, power, air conditioning used for data processing.
- People – qualifications, skills and experience in the use of information systems.
- Intangible – the ICB's reputation.

6.6.3 Essentially, it is information in any format that is of value to the organisation and would be problematic if it were not accessible.

6.6.4 Departments across the ICB are required to keep an Information Asset Register (IAR). The IG Team has processes and procedures in place to periodically request and review IARs and escalate any concerns to the SIRO. The ICB has clear lines of accountability for Information Risk Management (IRM) that reports directly to the Board through the SIRO.

Further information on this can be found within the Asset Management Policy and Business Continuity Policy.

6.7 Training Needs Analysis (TNA)

6.7.1 Staff holding specialist IG roles including, SIRO, Caldicott Guardian, DPO, IAOs and IAAs receive additional training commensurate with their role.

6.7.2 In IG TNA is developed, monitored and updated by the ICBs Head of Safe Practice as the DPO.

6.7.3 The need for any further IG training should be determined by line managers and their staff as part of the ICB's appraisal process.

6.8 Policies, Procedures & Staff Guidance

6.8.1 The ICB has a comprehensive range of IG Policies, procedures and staff guidance which support the IG agenda. These are listed under 'Associated Documents' on page 3. Legal and professional registration guidance should also be considered where appropriate.

6.8.2 Policies and guidance documents are available to all staff on the Staff Intranet. As part of the ICBs openness and transparency obligations the ICBs policies are also available on the ICBs public website Data Protection - BLMK Integrated Care Board

Appendix 1 - Equality Impact Assessment Initial Screening

Please answer the questions against each of the protected characteristic and inclusion health groups. If there are significant impacts and issues identified a full Equality / Quality Impact Assessment (EQIA) must be undertaken. It is against the law to discriminate against someone because of these protected characteristics. For support and advice on undertaking EQIAs please contact: agcsu.equalities@nhs.net

Name of Policy:	Information Governance Policy
Date of assessment:	1/9/2022
Screening undertaken by:	Head of Information Governance/DPO

Protected characteristic and inclusion health groups. Find out more about the Equality Act 2010, which provides the legal framework to tackle disadvantage and discrimination: Protected characteristics | EHRC	Could the policy create a disadvantage for some groups in application or access? (Give brief summary)	If Yes - are there any mechanisms already in place to mitigate the potential adverse impacts identified? If not, please detail additional actions that could help. If this is not possible, please explain why
Age A person belonging to a particular age (for example 32 year olds) or range of ages (for example 18 to 30 year olds).	No	
Disability A person has a disability if she or he has a physical or mental impairment which has a substantial and long-term adverse effect on that person's ability to carry out normal day-to-day activities.	No	
Gender reassignment The process of transitioning from one gender to another.	No	
Marriage and civil partnership Marriage is a union between a man and a woman or between a same-sex couple. Same-sex couples can also have their relationships legally recognised as 'civil partnerships'.	No	
Pregnancy and maternity Pregnancy is the condition of being pregnant or expecting a baby. Maternity refers to the period after the birth and is linked to maternity leave in the employment context. In the non-	No	

work context, protection against maternity discrimination is for 26 weeks after giving birth, and this includes treating a woman unfavourably because she is breastfeeding.		
Race Refers to the protected characteristic of race. It refers to a group of people defined by their race, colour and nationality (including citizenship) ethnic or national origins.	No	
Religion or belief Religion refers to any religion, including a lack of religion. Belief refers to any religious or philosophical belief and includes a lack of belief. Generally, a belief should affect your life choices or the way you live for it to be included in the definition.	No	
Sex A man or a woman.	No	
Sexual orientation Whether a person's sexual attraction is towards their own sex, the opposite sex, to both sexes or none.	No	
Carers Individuals within the ICB which may have carer responsibilities.	No	
Please summarise the improvements which this policy offers compared to the previous version or position.		
Reviewed to take into account ICB and new reporting mechanisms		
Has potential disadvantage for some groups been identified which require mitigation?		
No – (If there are significant impacts and issues identified a full Equality / Quality Impact Assessment (EQIA) must be undertaken.)		

Appendix 2 - Data Protection Impact Assessment Initial Screening

Data protection is the fair and proper use of information about people. Before completing this form, please refer to the Data Protection Impact Assessment (DPIA) Guidance in the Information Governance (IG) section on the staff Intranet or contact the Data Protection Officer for support via blmkicb.ig@nhs.net

A DPIA is a process to help you identify and minimise the data protection risks. You must do a DPIA for processing that is likely to result in a high risk to individuals. You can use our screening checklist below to help you decide when to do one. If you have answered 'Yes' to any of the 10 screening questions, you must then carry out a full DPIA using the Stage 2 form, which is also available on the Intranet in the IG section.

Name of Policy:	Information Governance Policy
Date of assessment:	14/03/2022
Screening undertaken by:	Head of Information Governance/DPO

Stage 1 – DPIA form **please answer 'Yes' or 'No'**

1.	**Will the policy result in the processing of personal identifiable information / data?** This includes information about living or deceased individuals, including their name, address postcode, email address, telephone number, payroll number etc.	Yes
2.	**Will the policy result in the processing of sensitive information / data?** This includes for living or deceased individuals, including their physical health, mental health, sexuality, sexual orientation, religious belief, National Insurance No., political interest etc.	Yes
3.	**Will the policy involve the sharing of identifiers which are unique to an individual or household?** e.g., Hospital Number, NHS Number, National Insurance Number, Payroll Number etc.	Yes
4.	**Will the policy result in the processing of pseudonymised information by organisations who have the key / ability to reidentify the information?** **Pseudonymised data -** where all identifiers have been removed and replaced with alternative identifiers that do not identify any individual. Re-identification can only be achieved with knowledge of the re-identification key. **Anonymised data -** data where all identifiers have been removed and data left does not identify any patients. Re-identification is remotely possible, but very unlikely.	No
5.	**Will the policy result in organisations or people having access to information they do not currently have access to?**	Yes
6.	**Will the policy result in an organisation using information it already holds or has access to, but for a different purpose?**	No
7.	**Does the policy result in the use of technology which might be perceived as being privacy intruding?** e.g., biometrics, facial recognition, CCTV, audio recording etc.	Yes
8.	**Will the policy result in decisions being made or action being taken against individuals in ways which could have a significant impact on them?** Including profiling and automated decision making. (This is automated processing of personal data to evaluate certain things about an individual i.e., diagnosis and then making a decision solely by automated means - without any human involvement)	No
9.	**Will the policy result in the collection of additional information about individuals in addition to what is already collected / held?**	No
10.	**Will the policy require individuals to be contacted in ways which they may not be aware of and may find intrusive?** e.g., personal email, text message etc.	Yes