NHS
Central East
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 Central East Integrated Care Board website is the controlled copy www.centraleast.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	Associate Director of Data Security and Information Risk (& Data Protection Officer)
Document Author(s)	Data Security & IG Officer
Directorate	Strategy, Planning and Evaluation
Approved By	CE ICB Board
Date of Approval	1.4.2026
Date of Next Review	31.3.2028
Effective Date	1.4.2026

Version Control

Version	Date	Reviewer(s)	Revision Description
1.0	1.4.2026	ICB Board	Aprpoved

Contents

1. Introduction

1.1 This policy sets out the principles and requirements for Information Governance Framework within NHS Central East Integrated Care Board (ICB). It aims to ensure a consistent and effective approach that supports the organisation's objectives, complies with statutory and regulatory requirements and promotes best practice.

1.2 The Information Governance (IG) Framework (the 'Framework') is a local framework of standards that bring together all statutory, mandatory and best practice requirements concerning information management and regulates the manner in which information (including information relating to and identifying individuals) is managed, i.e. obtained, handled, used and disclosed. This is based on national guidance, legislation and standards.

1.3 The standards are set out in the NHS England Data Security and Protection Toolkit (DSPT). The Data Security and Protection Toolkit is an online self-assessment tool that allows organisations to measure their performance annually. All organisations that have access to NHS patient data and systems must use this toolkit to provide assurance that they are practising good data security and that personal information is handled correctly.

The ICB's performance against these standards is mandated by and reported to NHS England and/or Department of Health and Social Care and forms a part of the assurance processes associated with the Care Quality Commission (CQC); NHS England (NHSE) and the NHS Resolution risk management standards.

2. Purpose and Scope

2.1 The purpose of this policy is to set out the overarching Framework of law and best practice for the strategic IG agenda and looks at the operational and management structures, roles, responsibilities, systems, policies and audit controls that the ICB intends to establish to ensure such issues are appropriately addressed throughout the organisation. This structured approach relies upon the identification of information assets and assigning 'ownership' of assets to senior accountable staff.

2.2 Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources. It plays a key part in Clinical Governance, service planning and performance management. It is therefore of paramount importance to ensure that information is effectively managed, and that appropriate policies, procedures and management accountability and structures provide a robust governance framework for information management.

2.3 This policy gives assurance to the ICB and to individuals that personal information is dealt with legally, securely, efficiently and effectively, in order to deliver the best possible care for our population. The policy and its supporting standards and instructions are fully endorsed by the ICB who will ensure that sufficient resources are provided to support its requirements.

2.4 This policy applies to all NHS Central East ICB staff, Board members, contractors, and others involved in working with patient/client/service user information, Personnel information and/or Organisational information, and any organisation or staff holding or processing data on behalf of the ICB.

3. Definitions

This section provides staff members with an explanation of terms used within this policy.

3.1 **Information Governance**

3.1.1 An umbrella term for a collection of distinct but overlapping disciplines. Information Governance is about the way in which the ICB handles its information, particularly personal data.

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 is the organisation that determines the use of personal data. They exercise the control over the purpose and means of processing.

3.3.2 The ICB is the Data Controller for the information it holds and is therefore responsible for compliance with data protection law and for ensuring organisations it shares information with or third parties who process information on its behalf have the appropriate technical and organisational measures in place to protect the information.

3.4 **Joint Data Controllers**

3.4.1 A joint Data Controller (also commonly described as Data Controller in common) will work together to determine the use and purpose of personal data and decide who will be take responsibility for each element of data protection law.

3.5 **Data Processor**

3.5.1 A Data Processor must act on the instruction from the Data Controller (including Joint Data Controllers). A Data Processor must be registered to process personal data with the Information Commissioner's Office (ICO) and be able to demonstrate that.

3.6 **Personal Data**

3.6.1 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.

A **Personal data breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

3.7 **Special Category Data**

3.7.1 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.

3.8 **Processing**

3.8.1 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.

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

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

3.9 Pseudonymised and Anonymised Information

3.9.1 It is important that staff understand the difference between anonymised and pseudonymised information (see below for definitions) as the level of security and risk is different for each.

3.9.2 Anonymised

Definition - *"...information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable." - Recital 26, United Kingdom General Data Protection Regulations (UKGDPR)*

In simple terms, information is unrecognisable and cannot be re-identified by referring to or linking it with other information which is available or likely to be available.

Information can only be classed as anonymised if all of the following have been removed and cannot be reverted back to its original form:

- Name
- Address
- Full postal code
- NHS number
- Date of birth
- Local identifiers (such as an employee number or hospital number)
- Anything else that could identify a patient for example a photograph, x-ray or dental records

3.9.3 Pseudonymised

Definition - *"…the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to*

technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person." - Article 4, UKGDPR

Pseudonymisation occurs when ALL identifiable e.g. name, address, NHS Number, Employee Number and any other unique identifier contributed to an individual has been replaced with alternative identifiers that bears no overt relationship to the true values which would identify an individual. Re-identification of data can only be achieved with knowledge of the de-identification key.

For example, in the situation where clinical trial data has had all identifiers removed, this can only be considered anonymised data if it is impossible to re-identify the trial subjects, even when cross referenced against supporting documentation.

Organisations frequently refer to personal data sets as having been 'anonymised' when, in fact, this is not the case. Staff must therefore ensure they consult

3.10 **Data Protection Impact Assessments**

Staff introducing changes must ensure that a Data Protection Impact Assessment is completed and approved before any changes are introduced especially where the processing of personal data is likely to result in a high risk to the rights and freedoms of individuals. A DPIA is an assessment of the impact of the envisaged processing operations on the protection of personal data'

3.11 **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).

3.12 **Department of Health and Social Care (DHSC)**

The Department of Health and Social Care helps people to live more independent, healthier lives for longer. It leads, shapes and funds health and social care in England, making sure people have the support, care and treatment they need, with the compassion, respect and dignity they deserve.

3.13 **Care Quality Commission (CQC)**

The CQC are the independent regulator of health and social care in England. They monitor and inspect health and social care services to ensure they provide people with safe, effective, compassionate, high-quality care and encourage care services to improve.

4. Policy Statement

4.1 NHS Central East ICB is committed to ensuring good quality information being available at the point of need in order to provide a high-quality service. Staff rely on the quality of data they use to make decisions about patient care and treatment, and the way in which we use resources and run ICB business. It is important for staff to understand their own responsibility for recording information to a consistently high standard and for keeping it secure and confidential. Public confidence in our ability to handle their data responsibly and efficiently is based on a good reputation for keeping their data safe.

4.2 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, both personal information about patients and staff and commercially sensitive information. The ICB recognises the need for an appropriate balance between openness and confidentiality in the management and use of information.

4.3 The ICB also recognises the need to share information with other health organisations and other agencies in a controlled and legal manner consistent with the interests of the patient and, in some circumstances, the public interest.

4.4 The ICB believes that accurate, timely and relevant information is essential to support the delivery of the highest quality health care. As such it is the responsibility of all clinicians and managers to ensure and promote the quality of information and to actively use information in decision making processes.

4.5 There are 4 key interlinked strands to the Information Governance Framework Policy:

- Openness and transparency;
- Legal compliance;
- Information security;
- Quality assurance.

4.6 <u>Legal Compliance</u>

- The ICB regards all identifiable personal information relating to patients as confidential;
- The ICB regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise;
- The ICB will undertake or commission annual assessments and audits of its compliance with legal requirements through the Data Security and Protection Toolkit;
- The ICB will establish and maintain policies to ensure compliance with the Data Protection Act; the Human Rights Act and the Common Law Duty of Confidentiality;

- The ICB will establish and maintain policies for the controlled and appropriate sharing of patient information with other agencies, taking account of relevant legislation (e.g. Health and Social Care Act, Crime and Disorder Act and Protection of Children Act)
- The ICB has a comprehensive range of information governance policies supporting the information governance agenda; reference must be made to these alongside this policy. Legal and professional guidance should also be considered where appropriate.

4.7 All staff are expected to adhere to the requirements set out in this policy.

5. Roles and Responsibilities

5.1 Senior Roles

5.1.1 Senior level ownership of information risk is a key factor in successfully raising the profile of information risks and to embedding information risk management into the overall risk management culture of the ICB. Senior leadership through the appointment of a Senior Information Risk Owner (SIRO) demonstrates the importance of ensuring information security remains high on the ICB's agenda.

5.1.2 Please see below a table outlining the senior roles in the ICB:

Accountable Officer	Chief Executive Officer
Senior Information Risk Owner (SIRO)	Executive Director of Strategy, Planning & Evaluation
Information Governance Lead	Head of Data Security & IG
Data Protection Officer (DPO)	Associate Director of Data Security & Information Risk
Caldicott Guardian	Executive Clinical Director – Utilisation Management
Cyber Security Lead	Information and Cyber Security Senior Manager

See **Appendix 3** for more details on Information Risk Roles and Responsibilities.

5.1.3 Information Governance Steering Group

The Steering Group has responsibility for the ICB's information governance performance and management with exceptions and assurance reported up to the Audit and Risk Committee (A&R).

5.2 Staff Responsibilities

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

5.2.2 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 ICB's IG policies and supporting guidelines.

5.2.3 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.

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

6. Processes and Procedures

The following processes must be followed to comply with this policy:

6.1 Information Governance Management and Oversight

6.1.1 The ICB's information governance performance and management are monitored through quarterly reporting to the ICB IG Steering Group with exceptions and assurance reported up to the Audit and Risk Committee (A&R). Individual items of action may be included within the Directorate's Risk Register for regular monitoring.

6.2 Data Security and Protection Toolkit (DSPT)

6.2.1 The annual information governance assessment is measured via an assessment process of compliance against the standards set out in the NHS DSPT and assured by Internal Audit.

6.2.2 The ICB is required to publish a DSPT baseline assessment and a final assessment by the 31 March annually with the objective of submitting a compliant 'Standards Met' toolkit.

6.3 Information Governance Training

6.3.1 Fundamental to the success of delivering the IG Policy and Management Framework is developing an Information Governance culture within the ICB. To promote this culture, awareness and training must be provided to all ICB staff (including staff on temporary contracts; secondments; agency workers and students) who utilise information in their day-to-day work.

6.3.2 All ICB staff complete Data Security Awareness Level 1 training annually on their Electronic Staff Record (ESR). Data Security Awareness training is incorporated into the ICB's schedule of mandatory training.

6.4 Training Needs Analysis

6.4.1 Staff holding specialist roles e.g. Senior Information Risk Owner (SIRO); Caldicott Guardian; Data Protection Officer; roles involve handling Personal Confidential Information; Information Asset Owners; Information Asset Administrators etc receive additional training commensurate with their role.

6.4.2 The frequency of any further information governance training will be determined as part of the ICB's organisation development plan and appraisal process.

6.5 Confidentiality of Personal Data

6.5.1 The Data Protection Act 2018 introduced additional levels of security around the processing of personal data. The ICB, as the legal entity and Data Controller for the purposes of the Data Protection legislation must ensure the **confidentiality** (information is accessible only to those who have a proven need to see it); **Integrity** (information held is accurate and up-to-date) and **availability** (information is there when it is needed to support care) of the personal data that we use.

6.5.2 The ICB will ensure that all personal data it holds is controlled and managed in accordance with relevant legislation.

6.6 Confidentiality Code of Conduct

6.6.1 All staff, whether permanent, temporary; contracted or voluntary who have been provided with privileged access to personal, confidential and or sensitive information are

responsible for ensuring that it is always handled in confidence. Staff must be aware of their individual responsibilities for the maintenance of confidentiality, data protection, information security management and information quality. Failure to maintain confidentiality may lead to disciplinary action, including dismissal.

6.7 Information Risk

6.7.1 The ICB establishes clear lines of accountability for information risk management that lead directly to the Integrated Care Board through the SIRO, DPO and the appointment of Information Asset Owners' (IAO) and Information Asset Administrators who are collectively responsible for the maintenance of a ICB wide Information Asset Register.

Additional information regarding specific roles and responsibilities can be found in Appendix 3.

6.7.2 Each Directorate is responsible for developing and maintaining a Directorate Risk Register in line with the organisational risk management policy which links into the ICB's Board Assurance Framework and Corporate Risk Register.

6.8 Incident Management

6.8.1 The ICB's SIRO and Caldicott Guardian via the relevant IAO must be informed immediately of all information security incidents involving the unauthorised disclosure of patient information for consideration of any necessary actions.

6.8.2 The incident reporting system is used for reporting, investigation and management of Information Governance and Information Security incidents and near misses. All information incidents reported on Datix will be reviewed by the IG Lead in accordance with NHS England's Incident Reporting Guidance to identify SI levels and reporting procedures. Relevant leads are identified for management and review of IG related incidents. Shared learning from incidents is disseminated via all staff email or staff bulletin as appropriate.

6.8.3 A key function of the IG Steering Group is to monitor and review untoward occurrences and incidents relating to Information Governance and to ensure that effective remedial and preventative action is taken. Reports of such incidents will be distributed to the Steering Group for consideration.

6.9 Data Protection Impact Assessments (DPIAs)

6.9.1 The impact of any proposed changes to the ICB's processes and / or information assets need to be assessed in accordance with the ICB's Data Protection Impact Assessment Policy and Procedure, to ensure that the confidentiality, integrity and accessibility of personal information are maintained.

6.9.2 The Data Protection Officer should be consulted during the design phase of any new service, process or information asset so that they can decide if a DPIA is required for a project or planned service change.

6.10 Information Asset Register

6.10.1 All Business Critical Information Assets including those that contain confidential data must be clearly identified on the ICB's Information Asset Register.

6.10.2 It is the responsibility of each IAO to identify what information assets are held within their area of responsibility, and to ensure this is documented in their Directorate's Information Asset Register which forms part of a ICB wide register managed by Data Security and IG Team.

6.10.3 The Information Asset Register should include all information necessary in order to recover from a disaster, including type of asset, format, location, backup information, license information, and a business value. The register should not duplicate other inventories unnecessarily, but it should be ensured that the content is aligned. In addition, ownership should be agreed and documented for each of the assets. Based on the importance of the asset, its business value and its security classification, levels of protection commensurate with the importance of the assets should be identified as should details of risk assessor, risk assessment frequency, risk assessment rating and date of last risk assessment.

6.10.4 There are many types of assets, including:

- **information:** databases and data files, contracts and agreements, system documentation, research information, user manuals, training material, operational or support procedures, business continuity plans, fallback arrangements, audit trails, and archived information;
- **software assets**: application software, system software, development tools, and utilities;
- **physical assets**: computer equipment, communications equipment, removable media, and other equipment;

- **services:** computing and communications services, general utilities, e.g. heating, lighting, power, and air-conditioning;
- **people** and their qualifications, skills, and experience;
- **intangibles** such as reputation and image of the organisation.

6.10.5 All information and assets associated with information processing facilities should be owned by a designated part of the organisation, for example a ICB Directorate. **Priority must be given to information assets that comprise or contain personal information about patients or staff.**

6.10.6 The IAO is responsible for ensuring that information and assets associated with information processing facilities are appropriately identified and classified; defining and periodically reviewing access restrictions, classifications, and business continuity arrangements taking into account applicable access control policies.

6.10.7 Routine tasks may be delegated, e.g. to a custodian looking after the asset on a daily basis (i.e. an Information Asset Administrator (IAA)), but the responsibility remains with the owner.

6.10.8 In complex information systems it may be useful to designate groups of assets, which act together to provide a particular function as 'services'. In this case, the service owner is responsible for the delivery of the service, including the functioning of the assets, which provide it.

6.11 Freedom of Information

6.11.1 The ICB uses all appropriate and necessary means to ensure that it complies with the FOI Act 2000 and associated Codes of Practice issued by the Lord Chancellor's Department pursuant to sections 45(5) and 46(6) of the Act. This is set out in the ICB's FOI Policy.

6.12 Records Management

6.12.1 The ICB is committed to a systematic and planned approach to the management of records within the organisation, from their creation to their ultimate disposal. The ICB ensures that it controls the quality and quantity of the information that it generates, can maintain that information in an effective manner, and can dispose of the information efficiently when it is no longer required. The ICB will ensure that Health Records are managed in accordance with Records Management Code of Practice 2020 as set out in the ICB's Records Management and Lifecycle Policy.

6.13 Information Quality Assurance

6.13.1 The quality of information acquired and used within the ICB is a key component to its effective use and management. As such, managers are expected to take ownership of, and seek to improve, the quality of data collected and held within their services.

6.13.2 The ICB:

- promotes data quality through the use of policies and procedures including the Records Management and Lifecycle Policy and Data Quality Policy and associated statutory professional requirements;
- undertakes or commissions annual assessments and audits of its arrangements in line with the Data Security and Protection Toolkit requirements;
- ensures that, wherever possible, information quality is assured at the point of collection;
- ensures that data standards are set through clear and consistent definition of data items in accordance with national standards.

6.14 Review of Contracts and Third-Party Contracts

6.14.1 Suitable clauses are included when negotiating and completing contracts with third parties who have access to or process personal information on behalf of the ICB. All contractors or support organisations with access to the ICB's information assets are clearly identified and appropriate information governance clauses included in their contracts. The terms and conditions of a contract ensure that failure to deliver any aspect of information governance assurances will be at the third party's risk. Attention must also be paid to the possible use of sub-contractors by the third party to provide services in order to undertake the contract.

6.14.2 It is not unusual to have third parties gaining access to the ICB's information assets, e.g. computers, telephones, paper records etc. The third parties include temporary agency staff, consultants, IT support staff etc. It is possible that as a result of access to information assets, third party staff may have access to patient or staff personal data. This situation therefore clearly has information governance risk implications such as data being used inappropriately.

6.14.3 The ICB maintains a register of all its contracts including third party contracts.

6.15 Contractual Risk Assessments

6.15.1 Directorates and IAOs should ensure that a risk assessment has been carried out prior to any agreement being made with a third party to evaluate any potential threats to information; networks; systems and locations from third party operatives. A DPIA must be used for this.

6.15.2 The ways in which third parties gain access, will help determine how extensive the risk assessment needs to be. For example, a risk assessment for cleaning contractors will be different to that carried out for a contractor connecting to the network. Temporary access will also see different considerations to long-term access.

6.16 Monitoring/Audit

6.16.1 The ICB will monitor this policy and related strategies, policies and guidance through the IG Steering Group.

- As assessment of compliance with requirements, within the Data Security and Protection Toolkit (DSPT) will be undertaken each year;
- The IG Steering Group will ensure implementation of the Data Security and Protection Toolkit (DSPT) Improvement Plan;
- An IG Annual report which will include a strategic plan for each work stream will be presented to the ICB's Integrated Performance and Assurance Committee;
- Internal Audit annual review is expected;
- The ICB will ensure that the support infrastructure for the SIRO and Caldicott Guardian is in place and kept under regular review.
- As part of the monitoring and compliance of this policy, we will do spot checks and monitor training compliance.

7. Statutory and National Guidance

7.1 This policy has been developed with reference to the following statutory and national guidance:

- United Kingdom General Data Protection Regulations (UKGDPR)
- Data Protection Act 2018 (DPA 2018)
- Data (Use and Access) Act 2025
- Access to Health Records Act (AtHR)1990
- Freedom of Information Act (FOIA) 2000
- Internation Information Security Standard: ISO/IEC 27002: 2005

- Caldicott Guidance
- Human Rights Act 1998
- Common Law Duty of Confidentiality
- Access to Medical Records Act 1990
- Copyright, Designs and Patents Act 1988 (as amended by the copyright computer programmed regulations 1992)
- Mental Capacity Act 2005
- Health and Social Care Act 2012
- Public Records Act 1958
- Protection of Children Act 1999
- Records Management Code of Practice for Health and Social Care 2016
- Electronic Communications Act 2000
- Communications Act
- Computer Misuse Act 1990
- Crime and Disorder Act 1998
- Information Security Management: NHS Code of Practice 2007
- Regulations of Investigatory Powers Act 2000 (RIPA)
- Privacy and Electronic Communications Regulations (PECR) 2003

7.2 The ICB regards all identifiable personal information relating to patients as confidential.

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

7.4 The ICB will undertake or commission annual assessments and audits of its compliance with legal requirements through the Data Security and Protection Toolkit.

7.5 The ICB will establish and maintain policies to ensure compliance with the Data Protection Act; the Human Rights Act and the Common Law Duty of Confidentiality.

7.6 The ICB will establish and maintain policies for the controlled and appropriate sharing of patient information with other agencies, taking account of relevant legislation (e.g. Health and Social Care Act, Crime and Disorder Act and Protection of Children Act)

7.7 The ICB has a comprehensive range of information governance policies supporting the information governance agenda; reference must be made to these alongside this policy. Legal and professional guidance should also be considered where appropriate.

8. Stakeholder Engagement Record

8.1 The following stakeholders were engaged in the development of this policy:

Role/Group	Date of Engagement	Summary of Feedback
Joint IG Steering Group	16th March 2026	Changes made, ready for Board Approval.
CEICB Board	1st April 2026	TBC

Accessibility Statement

This policy is available in alternative formats upon request, including large print, Braille and translated versions, to ensure accessibility for all staff and stakeholders.

Implementation Plan

Development and Consultation: The following individuals were consulted and involved in the development of this document:

- Information Governance Team
- Joint IG Steering Group

Dissemination: Staff can access this document via the staff website and will be notified of new/revised version via the internal staff newsletter.

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 complete and pass the NHS Data Security Awareness training on an annual basis.

Monitoring: Monitoring and compliance of this document will be carried out via:

- An assessment of compliance regarding information sharing is undertaken within the Data Security and Protection Toolkit, each year and audited by internal auditors.
- In addition, the ICB's Data Security & IG Team 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.

Equality, Diversity, and Privacy: See Appendices

Associated Documents: The following documents must be read in conjunction with this document:

- Information Sharing Policy
- Data Protection Policy
- Access to Records Policy
- Records Management & Lifecycle Policy
- ICB Privacy Notice

NHS
Central East
Integrated Care Board

Appendix 1: Equality Impact Assessment

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 Framework
Date of assessment:	February 2026
Screening undertaken by:	Data Security & IG Officer

Protected characteristic and inclusion health groups. **Find out more about the Equality Act 2010, which provides the legal framework to tackle disadvantage and discrimination:** **https://www.equalityhumanrights.com/en/equality-act/protected-characteristics**	**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-work context, protection against maternity discrimination is for 26 weeks after giving birth, and this includes treating a woman unfavourably because she is breastfeeding.	No	
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	No	

Whether a person's sexual attraction is towards their own sex, the opposite sex, to both sexes or none.		
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.		
N/A		
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.)		

NHS
Central East
Integrated Care Board

Appendix 2: Data Protection Impact Assessment

Screening questions to determine if a full DPIA is required. Guidance on handling personal and sensitive data.

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 ***(insert email address once confirmed)***

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 Framework
Date of assessment:	February 2026
Screening undertaken by:	Data Security & IG Officer

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

Appendix 3: Data Security, Information Risk and Information Governance Roles and Responsibilities

The Chief Officer

The Chief Executive Officer as the Accountable Officer for the ICB has overall accountability and responsibility for Information Governance within the ICB and is required to provide assurance through the Statement of Internal Control that all risks to the organisation, including those relating to information, are effectively managed and mitigated.

The Senior Information Risk Owner (SIRO)

The Director of Strategy and Planning at the ICB is the SIRO with overall responsibility for managing information risk across the organisation and is the owner of the ICB's Information Asset Register. The SIRO is a member of the Integrated Care Board and provides written advice to the Accountable Officer on the content of the Annual Governance Statement and the Statement of Internal Control in regard to information risk. ,

The SIRO is responsible to the Board for ensuring that all Information risks are recorded and mitigated where applicable. The SIRO is responsible for ensuring that all record management issues (including electronic media) are managed in accordance with this Framework.

The SIRO owns the ICB's overall information risk assessment process, tests its outcome, and ensures it is used. The SIRO is responsible for how the organisation implements NHS Information Governance risk management in its own services and activities and those of its delivery partners, and how compliance is monitored. The SIRO ensures that quarterly information asset risk reviews are completed. Based on the information risk assessment the SIRO evaluates the information risks to the organisation and its business partners through its delivery chain, and ensures that they are addressed, and that they inform investment decisions including the risk considerations of outsourcing.

The SIRO is supported by Information Asset Owners, the ICB's Caldicott Guardian and members of the ICB Steering Group, although ownership of Information Risk and the information risk assessment process remains with the SIRO.

<u>Key Responsibilities of the Senior Information Risk Owner (SIRO)</u>

- To oversee the development of an Information Risk Policy, and a Strategy for implementing the policy within the existing Information Governance Framework;

- To take ownership of the risk assessment process for information risk, including review of the annual information risk assessment to support and inform the Statement of Internal Control;
- To review and agree an action plan 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 Officer and the Board on information risk management strategies and provide periodic reports and briefings on progress.

Caldicott Guardian

The Executive Clinical Director is the ICB's Caldicott Guardian and the 'conscience' of the organisation, providing a focal point for patient confidentiality and information sharing issues and advising on the options for lawful and ethical processing of information as required.

Key responsibilities of the Caldicott Guardian

- Strategy and Governance: The Caldicott Guardian champions confidentiality issues at Integrated Care Board/executive management team level and sits on an organisation's Information Governance Committee/Group and acts as both the 'conscience' of the organisation and as an enabler for appropriate information sharing.
- Confidentiality and Data Protection expertise: The Caldicott Guardian develops a strong knowledge of confidentiality and data protection matters, drawing upon support staff working within an organisation's Caldicott and information governance functions, but also on external sources of advice and guidance where available.
- Internal information processing: The Caldicott Guardian ensures that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff. The key aspects that need to be addressed by the organisation's Caldicott function were detailed in the Information Governance Toolkit up to March 2018 and these remain embedded as good practice.
- Information sharing: The Caldicott Guardian oversees all arrangements, protocols and procedures where confidential personal information is shared with external bodies and others with responsibilities for 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.
- Caldicott training is required to be undertaken every other year.

Data Protection Officer (DPO)

The Data Protection Officer provides the organisation with independent risk-based advice to support its decision-making in the appropriateness of processing Personal and Special Categories of Data within the Principles and Data Subject Rights laid down in the General Data Protection Regulation (GDPR).

Key responsibilities of the Data Protection Officer (DPO)

The Data Protection Officer (DPO) is responsible for monitoring compliance with data protection law and ensuring data practices internally comply with applicable requirements and serves as the primary contact for supervisory authorities and individuals whose data is processed by the organisation.

The DPO is an essential role in facilitating 'accountability' and the organisations ability to demonstrate compliance with the GDPR. The organisation must appoint a DPO whose job description is compliant with GDPR requirements and in particular must ensure:

- that the DPO role directly reports 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;
- that the DPO role is provided with adequate resources: financial and human resources, and is supported in maintaining his or her expertise;
- that the DPO has proven 'expert knowledge of data protection law and practices', the ability to perform the tasks specified in the GDPR, and sufficient understanding of the organisation's business and processing;
- that information governance and related policies address organisational accountability;
- DPO reporting arrangements;
- timely involvement of the DPO in all data protection issues;
- compliance assurance: privacy by design and default advising on where data protection impact assessment is required;
- the DPO's role in incident management;
- that the DPO does not receive any instruction regarding the exercise of his or her tasks, and is protected from disciplinary action, dismissal or other penalties;
- that where the DPO performs another role or roles, that there is no conflict of interest;
- that the contact details of the DPO are published in the ICB's transparency information for subjects and are communicated to the ICO.

Head of Data Security & IG

The Head of Data Security & IG's role is to ensure that the ICB has a managed and co-ordinated approach to the implementation of Information Governance within the organisation so that it is able to meet both its statutory and legal obligations. The IG Lead provides support and guidance to the ICB's Caldicott Guardian and SIRO roles and works closely with them to

develop and monitor the annual IG work programme to feed into the Governance Directorate's Annual Development Plan.

Key Responsibilities of the IG Lead, including but not limited to:

- Lead on Information Governance for the ICB.
- Define, develop, and improve multi-agency information sharing through technology and in line with Data Protection and Caldicott guidelines.
- Ensure commissioning ICB is compliant with information governance requirements and management standards.
- Ensure that the ICB has robust systems in place for information governance that comply with legislative and other requirements (Freedom of Information Act, Data Protection, Caldicott etc.), working with shared services.
- Develop organisational policies and processes to support information governance requirements.
- Ensure that IG is integrated into the core business functions and organisational plans and strategy of the ICB.
- Agree audit plans in relation to IG with external and internal auditors and ensure management action plans are developed, implemented and monitored in response to audit recommendations.
- Provide information governance advice when requested to ICB staff members; Primary Care and raise awareness of standards and requirements to independent contractor clinicians.
- Provide information and advice on IG outcomes and implications for governance, performance, assurance and risks across the organisation.

Data Security & IG Senior Manager

The Data Security & IG Senior Manager works closely with the Information Governance Lead to ensure that national and ICB requirements are met, with particular responsibility for capturing and analysing information from the following work streams for governance scrutiny:

Key Responsibilities of the Data Security & IG Senior Manager including but not limited to:

- Project management of the ICB's annual baseline and final Data Security and Protection Toolkit submissions.
- Review developments to the Data Security Awareness Training portal and ensure implementation as part of the mandatory annual requirement of staff training.
- Support the ICB C&I, A&G Steering Group.
- Project Support to the Information Governance Lead.
- Management of IG incidents and risks.
- Develop staff training content and awareness of Information Governance matters.

- Develop policy and procedure to meet the Data Security and Protection Toolkit requirements, project managing the ICB's annual baseline and final DSPT submissions to NHS England, ensuring timely publication.
- Produce and implement Information Governance action plans in line with the Toolkit, internal and external audit and national requirements.
- Work in collaboration with the appropriate teams to ensure that IG standards are built into all projects, business cases and performance monitoring.

Information Asset Owner (IAO)

Information Asset Owners (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 'own'. IAOs also lead and help foster, within their respective Directorates, a culture that values, protects and uses information. IAOs must be a member of staff senior enough to make decisions concerning the asset at the highest level. All the ICB's IAOs are members of the Board involved in running the Organisation. Their role is also to understand and assess risks to the information assets they 'own' 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 the ICB's Information Asset Register.

The owner can assign day to day responsibility for each information asset to an administrator or manager known as an Information Asset Administrator, which must be formalised in job descriptions.

The SIRO is responsible for the appointment and management (in terms of information assets) of the IAOs.

<u>Key Responsibilities of the IAO</u>

To understand and address risks to the information assets they 'own' and provide assurance to the SIRO on the security and use of these assets (understands the ICB's plans to achieve and monitor the right NHS IG culture, across the ICB and with its business partners and to take visible steps to support and participate in that plan (including completing own training).

Working closely with the Data Protection Officer and Information Governance Manager, IAO's will take appropriate actions to:

- Know what information the Asset holds and understands the nature and justification of information flows to and from the asset (approves and minimises information transfers while achieving business purposes; approves arrangements so that information put onto portable or removable media like laptops is minimised and are effectively protected to NHS IG standards.

- Know who has access and why, and ensure their use is monitored and compliant with policy (checks that access provided is the minimum necessary to satisfy business objectives; receives records of checks on use and assures self that effective checking is conducted regularly).
- Ensure the confidentiality, integrity, and availability 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 for all new projects in line with the ICB's Data Protection Impact Assessment Policy and Procedure.
- Participate in an Annual Information Risk Assessment.
- Understand and address risks to the asset and provide assurance to the SIRO (makes the case where necessary for new investment or action to secure 'owned' assets; provides an annual written risk assessment to the SIRO for all assets 'owned' by them).
- Ensure that information risk assessments are reviewed at least once every quarter on all information assets where they have been assigned 'ownership' and where:
    - New systems, applications, facilities etc. is introduced that may impact the assurance of ICB Information or Information Systems;
    - Before enhancements, upgrades, and conversions associated with critical systems or applications;
    - Ensure that all high risks follow the ICB's process for inclusion on the ICB's Assurance Framework and Risk Register.
- IAOs shall submit the risk assessment results and
- associated mitigation plans to the SIRO for review. Mitigation plans shall include specific actions with expected completion dates, as well as an account of residual risks;
- Compile their Information Asset Register.
- Ensure the asset is fully used for the benefit of the organisation and its patients, including responding to requests for access from others (considers whether better use of the information is possible or where information is no longer required; receives, logs and controls requests from others for access; ensures decisions on access are taken in accordance with NHS IG standards of good practice and the policy of the organisation.
- Approve and oversee the disposal mechanisms for information of the asset when no longer needed).
    - At least once a year, each of the ICB's IAOs will carry out a risk assessment to examine forthcoming potential changes in services, technology and threats and provide assurances to the ICB's SIRO on the security and use of assets they 'own'. All high risks are escalated to the Integrated Care Board via the ICB Assurance Framework and Risk Register.

Information Asset Administrator (IAA)

Information Asset Owners (in consultation with the SIRO) 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. Information Asset Administrators are operational staff with day to day responsibility for managing risks to their information assets. They will support IAOs by ensuring that policies and procedures are followed, recognise actual or potential security incidents, consult their IAO on incident management, ensure that data protection impact assessments are completed and ensure that information asset registers are accurate and up to date.

Key Responsibilities of the IAA

Information Asset Administrators will provide support to their IAOs to ensure that policies and procedures are followed and to recognise potential or actual security incidents. They will consult their IAOs on incident management to ensure that information asset registers are accurate and maintained up to date.

Ensuring compliance with data sharing agreements within the local area 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 exploited, 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.