NHS
Central East
Integrated Care Board

Data Protection Policy

NHS
Central East
Integrated Care Board

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	Approved

Contents

1. Introduction

1.1 This policy sets out the principles and requirements for Data Protection 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 NHS Central East ICB is committed to the delivery of a first-class confidential service in accordance with the law, regulatory standards, and service user expectations. This means ensuring that all information is processed fairly, lawfully, and as transparently as possible so that patients and the public:

- understand the reasons for processing personal information.
- gain trust in the way we, as ICB of publicly funded health and social care services handle information, and;
- understand their rights under the relevant legislation.

1.3 Readers of this policy are encouraged to remember that we are all users of health and social care services and to consider the fairness, respect and confidentiality with which they would want their own records to be processed. It is impossible for policies to cover every eventuality and therefore readers should use reasonable judgement in decisions on using and communicating confidential information and ask for advice if needed.

2. Purpose and Scope

2.1 The purpose of this policy is to ensure that all individuals to whom this policy relates are aware of their obligations and responsibilities regarding confidentiality, compliance with legislation and guidance and are aware of the consequences of breaches of confidentiality for individuals and for themselves, and to support confidence in day to day handling (processing) of personal data.

2.2 This policy relates to the processing of person identifiable data and mainly refers to patient and service user information; however, the principles apply to any use of person-identifiable data (such as human resources (HR) and staff data).

2.3 The principles of confidentiality also apply to confidential business activities (e.g., tendering processes, commissioning new services and performance management).

2.4 All staff must meet the standards outlined in this document as well as other relevant NHS Codes of Practice. They will have contracts of employment, professional registration body regulations and further ICB policies and confidentiality agreements that they must sign up to.

2.5 This policy applies to all NHS Central East ICB staff, Board members, contractors, and others (inc. students, volunteers etc) who have access to ICB systems, or patient, staff and/or organisation-confidential or business sensitive information and have a duty of confidence to 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 compliance with relevant data protection legislation, legal obligations and NHS standards that are placed upon the ICB for the processing of personal identifiable information. These are listed in the ICBs IG Framework Policy (which must be read in conjunction with this policy).

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

5. Roles and Responsibilities

5.1 The following have specific responsibilities in relation to this policy:

5.1.1 **Senior Information Risk Owner (SIRO)**
The Senior Information Risk Owner (as Executive Lead) has overall responsibility for the Data Protection Policy.

5.1.2 **Caldicott Guardian (CG)**
The Caldicott Guardian has responsibility for placing appropriate controls and procedures for monitoring access to any person identifiable data held by the ICB.

5.1.3 **Data Protection Officer (DPO)**
The Data Protection Officer (DPO), will be responsible for providing advice, liaising with other organisations to process subject access requests, co-ordinating the release of the data and investigating complaints and summary care record alerts.

5.1.4 **Data Security and Information Governance Team (IG)**
The Data Security and Information Governance Team (IG) will oversee the annual review of the Data Protection Policy and make amendments in line with UKGDPR requirements and raise any issues with compliance to the IG Steering Group.

ICB Information Governance Steering Group

The ICB's IG Steering Group will escalate issues with compliance to the Audit and Risk Committee, who have final sign off on the policy.

5.1.5 **Information Asset Owners (IAOs)**
Information Asset Owners are responsible for ensuring that all records that include person identifiable data are included in the directorate information asset register, are regularly reviewed (at least annually) and reporting any risks to the Senior Information Risk Owner (SIRO).

5.1.6 **Information Asset Administrators (IAAs)**
Information Asset Administrators (IAAs) are responsible for ensuring that records containing person identifiable data are added to the directorate information asset register and that risks are reported to the Information Asset Owner (IAO).

5.1.7 **Managers/Heads of Departments**

All Managers/Head of Departments 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.

5.2 All Staff responsibilities

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

Staff should note that there is 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 guidance documents.

Any breach of confidentiality, inappropriate use of information or abuse of computer systems may result in disciplinary action which could result in dismissal/termination of contract and/or legal action being taken.

5.2.1 Training

All staff must complete Data Security Awareness training on an annual basis. Compliance is monitored monthly and a reminder sent to those members of staff whose training is about to, or has, expired.

5.2.2 Accuracy of data

All staff are responsible for ensuring that:

- Their own personal data in relation to their appointment is accurate and up to date
- Person identifiable data that they handle lawfully as part of their role is as accurate and up to date as possible, kept securely with restricted access and not kept for longer than necessary.

5.2.3 Methods of Communication

Staff should be aware that the Data Protection Act (DPA) and GDPR applies to all communication methods including emails, text messages, MS Teams messages etc, sent or received for ICB purposes.

5.2.4 Security of data

All staff are responsible for ensuring that personal or sensitive data is held securely and that it is not disclosed to any unauthorised third party. Data that is disclosed inappropriately or accidentally must be reported using the ICBs online incident reporting system. Major breaches of confidentiality or data loss should be reported to their line manager and the IG Lead/DPO in the first instance.

5.2.5 Retention of data

The Data Protection Act requires that data be not held for longer than necessary. Staff are required to identify the retention periods for all personal data held by them and ensure that it is disposed of securely in accordance with retention and destruction guidelines included in the Records Management Code of Practice.

6. Processes and Procedures

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

6.2 Data Protection Registration

6.2.1 The ICB has a responsibility to register with the ICO. The IG Lead manages the notification on behalf of NHS Central East ICB. Monitoring of the information asset register and data flow mapping will be carried out on an annual basis to ensure the registration is kept up to date.

6.3 Contracts and Service Level Agreements

6.3.1 The ICB must ensure that appropriate wording regarding compliance with the Data Protection Act and GDPR is covered in all contracts and service level agreements before these are signed or changes are agreed. Temporary staff, students, volunteers and contractors are required to sign a confidentiality agreement.

6.4 Legal Basis for Processing

6.4.1 Personal identifiable information must not be processed unless there is a legal basis as listed in UKGDPR under Article 6 – Legal Basis for Processing Personal Information– see Appendix 3.

6.4.2 In addition, where the information is special category information an additional legal basis must be identified as listed in UKGDPR under Article 9 – Processing of special categories of personal data – see Appendix 3.

6.4.3 When considering new processing or change of purpose for which a legal basis needs to be identified staff must consult the ICBs Data Security & IG Team for advice and support.

6.4.4 Further information can be found in our Privacy Notice.

6.5 Data Protection Principles

6.5.1 Article 5 of the UKGDPR sets out 7 basics '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.

6.5.2 Lawfulness, Fairness and Transparency (Principle a)

'Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject'

This means there must:

- be a legal basis for collecting, using and sharing personal and/or sensitive information and,
- fairness and transparency about what information will be used for.

The ICB complies with the requirement of fairness and transparency by publishing fair processing information (known as a Fair Processing Notice) on the ICB public website.

The ICBs DPO reviews the notice on a yearly basis to ensure it remains accurate and up to date.

6.5.3 Purpose Limitation (Principle b)

'Personal data shall be obtained for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes'

The purposes for which personal information about living Data Subjects is obtained, held, and/or processed by the ICB, must be registered with the ICO. It is the responsibility of the DPO to submit an appropriate notification for the ICB on an annual basis and to ensure the notification is accurate. The notification must be updated with any relevant changes.

Information held by the ICB must only be used for the purpose for which it was collected, and any additional use can only be authorised with the specific permission/consent of the data subject(s) concerned.

For help with assessing the risks associated with processing information staff MUST contact the ICB's Data Security & IG Team.

6.5.4 Data Minimisation (Principle c)

'Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed'

Commonly known as the adequacy principle, it obliges the ICB, as Data Controller, to obtain only the minimum information that is necessary for the purpose, or purposes, of processing the data.

Consideration of the format of information must also be included here with only the lowest level of information used, these formats are;

- Clear Data (fully identifiable information).
- Pseudonymised
- Anonymised
- Aggregated – where the data is in groups only and cannot be identified down to a Data Subject.

Staff should consider the minimum level of information required and the format that these could be provided or processed in.

6.5.5 Accuracy (Principle d)

'Personal data shall be accurate and, where necessary, kept up to date'

All ICB staff who collect personal identifiable information about individuals from individuals have a duty to check and ensure the information is accurate and up to date.

In addition, information held on paper MUST be available to those who need it, when it is needed. This is particularly relevant when it comes to information being used to deliver direct care or to protect/safeguard and individual.

Staff also have a duty to inform their line manager of any changes to their personal information e.g. change of address etc.

6.5.6 Storage Limitation/Retention (Principle e)

'Personal data processed for any purpose or purposes shall not be kept longer than is necessary for that purpose or those purposes'

All information should be stored, retained and destroyed in line with the ICBs Records Management & Lifecycle Policy (based upon the NHS Records Management Code of Practice).

Where any records are required to be retained beyond the minimum period, this must be discussed with the ICB's DPO.

6.5.7 Integrity and Confidentiality (Principle f)

'Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures'

This principle is also known as the security principle.

To ensure the safety and integrity of all personal data the ICB is required to take steps to put in place technical solutions to protect information. These are covered in the ICB's IT Security Policies, which staff are required to comply with.

All staff with access to the ICB's network and systems, regardless of where they are working e.g., in the office or offsite, must take adequate precautions to ensure confidentiality so that neither the ICB, nor any Data Subject employed by the ICB, become exposed to criminal activity as a result of the loss, destruction or disclosure of their information.

When information is processed by a 3rd party Data Processor on behalf of the ICB, staff must ensure a contract is in place and that it states that the Data Processor can act only on instructions from the ICB. The contract must also require the 'Data Processor' to comply with obligations equivalent to those imposed on the Data Controller.

Staff entering into contracts with third parties must consult with the Contracts Department and the IG Team.

6.5.8 Accountability Principle

Article 5(2) GDPR - 'Accountability' is the 7th data protection principles. It requires the ICB to put appropriate technical and organisational measures in place to meet the requirements of UKGDPR, in particular principles a to f as listed above.

The ICB has a number of measures in place including:

- IG & data protection policies as listed in this policy.
- IG & data protection procedures and guidance.
- A privacy by design and default approach – see Data Protection Impact Assessment (DPIA) section below.
- Written contracts in place with organisations that process personal data on the ICBs behalf.
- Maintaining documentation of the ICBs processing activities, including the legal basis for each activity.
- Recording, investigating, learning from and where necessary, reporting personal data breaches.
- Appointment of a DPO as detailed above.

- Requirement for a process in place for all staff to complete the Data Security & Protection staff training on ESR as part of Mandatory Training.
- Fair Processing Notices (the right to be informed) – see Appendix 5.

6.6 Rights of the Data Subject

6.6.1 UKGDPR sets out specific rights for data subjects. Not all of these rights will apply to every individual; this will depend on the legal basis used to collect and process the information. Further detail can be found within Appendix 5.

- The Right of Access (Subject Access Request (SAR))
- 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

6.6.2 Staff must refer any enquiries about these rights to the Data Security & IG Team immediately.

6.7 Asset Register

6.7.1 All records containing person identifiable data should be identified in the directorate asset register and a lawful basis for processing cited. This includes all data held in electronic and paper form. The asset register should be reviewed at least annually by the information asset administrators and updates reported to the information asset owners.

6.7.2 Systems, services and processes (paper based, and electronic) which process information should have a designated IAO (and, in some cases, one or more IAAs). The role of the IAO is to understand what information is held within the system or is being transferred through processes, what is added and what is removed, methods of information transfer, and who has access to the system(s) and why.

6.8 Changes to systems and processes

6.8.1 It is important that changes to services and systems and processing of person identifiable data are assessed to ensure that confidentiality, accessibility, and integrity of

data are maintained. 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'.

6.9 Personal Data Breaches

6.9.1 Part 3 of the Data Protection Act introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority (ICO). Where feasible, incident reporting to the ICO should be within **72 hours** of an organisation becoming aware of the breach. Once you become aware of a breach, where feasible, report to the Data Security and IG Team within 24 hours.

6.9.2 If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, affected individuals must be informed without undue delay.

6.9.3 Organisations are required to have robust breach detection, investigation, and internal reporting procedures in place.

6.10 Disclosure outside of the UK

6.10.1 Personal data, even if it would otherwise constitute fair processing, must not, unless certain exemptions apply or protective measures taken, be disclosed or transferred outside the UK to a country or territory which does not ensure an adequate level of protection for the rights and freedoms of data subjects. Advice should be sought from the IG Lead/DPO or Caldicott Guardian before any such information is transferred.

6.11 Sharing Information

6.11.1 Please refer to the ICB Information Sharing Policy for full details of when and how information sharing is appropriate/allowed, and responsibilities. For ease of use, this section provides a summary:

6.11.2 <u>Sharing for direct care – consent model</u>

In accordance with the Common Law Duty of Confidentiality, data protection legislation and various codes of best practice and conduct, the ideal situation when Personal Confidential Data (PCD) may be legitimately shared is that the person whose information it is (or their legal representative, e.g., parents for children, person with Power of

Attorney for Health & Welfare) has freely given informed explicit consent to information being shared.

Consent is not the only lawful basis for sharing: Caldicott Principle 7; section 3 of the Health & Social Care (Quality & Safety) Act 2015 and (from 25 May 2018, UKGDPR Article 9(2)(h)) provide a lawful basis for sharing information with members of a service user's direct care team, for the sole purpose of providing them with care. This should not be defined as implied consent: the principle is one of reasonableness and 'no surprises' for the person whose information is being shared. Consent must not be obtained if there is no 'choice' except to share information. For example, if someone consents to a referral, then this can be understood as consenting to information being shared as relevant to that referral, and there is a lawful basis for this.

Separate consent for sharing information should not be asked.

Individuals should always be informed about how their information will be shared. Continuing with the referral example, a clinician may tell the individual that they need to include information about other health conditions / co-morbidities as well as the health condition for the referral being made.

Data Sharing agreements do not permit unrestricted access to PCD: they set the conditions for safe and secure sharing where there is a legitimate purpose for doing so.

6.11.3 Sharing without consent

Situations where consideration of disclosure of information without explicit consent include:

- Between health and social care professionals who are directly involved in the individuals' care for the purposes of provision of the highest quality care in accordance with principles section 6. *Note: All electronic sharing of personal confidential data should always be through a secure route i.e., NHS net to NHS net; encryption.*
- In the public interest – e.g., the Public Health (Control of Disease) Act 1984 and the Public Health (Infectious Diseases) Regulations 1988 require the notification of certain diseases to the local authority.
- For the detection and prevention of serious crime or where it is necessary to fulfil a statutory obligation or court order. The Police do not necessarily have any legal right of immediate access to PCD. Please see the ICB Access to Records Policy for more detail.
- For safeguarding purposes – protection of a vulnerable child or adult from abuse or neglect. Refer to the ICB's Safeguarding Leads and policies.
- Where there is a risk of serious harm to an individual or others: health and safety issues for staff (e.g., environmental factors, violent patients) must be referred to the

Local Security Management Specialist or Corporate Services Manager as appropriate.

- Where the person lacks the capacity to make a particular decision to take a particular action for themselves, at the time the decision or action needs to be taken. This would include decisions about the sharing of information – see Mental Capacity Act 2005, Chapter 16

6.11.4 Access to records or sharing for non-direct care purposes (secondary use)

Service user information may need to be accessed or shared for non-care purposes. In some cases, (e.g., clinical audit, Care Quality Commission quality inspections) there may be a lawful basis for staff and other authorised individuals to access records/PCD in accordance with performance and monitoring requirements in health and social care legislation.

In all other cases, if identifiable service user information for one or more users, is to be shared for non-care purposes, research and evaluation processes, or for any other non-care use (for example, service redesign), please refer to the ICB Information Sharing Policy.

In the event of any uncertainty or concern about sharing PCD the final decision on disclosure will be made by the DPO (and/or the ICB's Caldicott Guardian, as appropriate).

6.11.5 National data opt-out

The national data opt-out was introduced on 25 May 2018, enabling patients to opt out from the use of their data for research or planning purposes, in line with the recommendations of the National Data Guardian in her Review of Data Security, Consent and Opt-Outs.

Patients can view or change their national data opt-out choice at any time by using the online service at www.nhs.uk/your-nhs-data-matters.

By 2020 all health and care organisations are required to be compliant with the national data opt-out policy. NHS England and Public Health England are already compliant and are applying national data opt-outs.

6.12 Transfers of Personal Information outside the UK

6.12.1 The Data Protection Act governs transfers of personal information and requires that personal information is not transferred to countries outside of the European Economic Area (EEA) unless that country has an adequate level of protection for the information and for the rights of individuals. The EEA is made up of the EU member states plus the European Free Trade Association (EFTA) countries of Iceland, Liechtenstein and Norway. All transfers of personal data outside the EEA must be for a lawful and justified purpose and the ICB's Caldicott Guardian must be informed of such transfers. A log of such transfers must be maintained.

6.12.2 Personal Information should only be transferred outside the EEA if the individual's consent, which should be explicit, has been obtained or following a risk assessment the Caldicott Guardian is satisfied that there is an adequate level of protection in place. In certain circumstances a contract containing standard EU approved clauses as providing adequate protection to transfer individuals' personal information may be necessary.

6.13 Privacy and Fair Processing Notice

6.13.1 As data controllers, the ICB is required to provide certain information to people whose information (personal data) is held and used. The ICB does this by providing information to its staff via the Extranet and to the public via the ICB's Privacy and Fair Processing Notice on the ICB website. The privacy notice identifies who the ICB is, what they do and provides contact details for the ICB's Data Protection Officer. The ICB must also explain the purposes for which personal data are collected; used; disclosed; how long it is kept and the legal basis for processing.

6.13.2 The ICB is committed in ensuring that individuals are adequately informed about confidentiality and their rights as data subjects, in particular how they may contact the ICB about or to access their personal data.

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
- Data (Use and Access) Act 2025
- Common Law Duty of Confidentiality

- Access to Health Records Act 1990
- Freedom of Information Act 2000
- The Mental Capacity Act (2005)
- Human Rights Act 1998
- Health & Social Care (Safety & Quality) Act 2015
- Caldicott Committee Report of the Review of Patient-Identifiable Information 1997
- The Information Governance Review ('Caldicott 2') April 2013
- NHS Care Record Guarantee - Information governance for Summary Care Records (SCR) - NHS England
- The NHS Code of Practice on Confidentiality (2003)
- 'A guide to confidentiality in health and social care' Health & Social Care Information Centre September 2013

7.2 **Further Guidance**

If you have any concerns or issues with the contents of this policy or have difficulty understanding how this policy relates to you and/or your role it is important that you seek clarification. Please raise concerns and queries with your line manager.

The Safeguarding Team can advise on safeguarding-specific queries.

The Data Security and IG Team can advise on more complex situations and will consult with the Caldicott Guardian and Data Protection Officer as required.

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	

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
- Information Governance Framework 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:	Data Protection Policy
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	No	

gender to another.		
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 – Initial version		
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:	Data Protection Policy
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.	No
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.	No
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.	No
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?	No
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.	No
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.	No

Appendix 3: Lawful Bases for Processing Personal Data

Article 6 – Legal Basis for Processing Personal Information
The lawful bases for processing Personal data are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

a) **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.

b) **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

c) **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations)

d) **Vital interests:** the processing is necessary to protect someone's life.

e) **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

f) **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Article 9 – Legal Basis for Processing Special Category Information
The lawful bases for processing Special Category data are set out in Article 9 of the GDPR. At least one of these must apply whenever you process special category data:

a) **Explicit Consent** - the data subject has given explicit consent to the processing of those personal data for one or more specified purposes,

b) **Obligations o/ Specific Rights** - processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law.

c) **Vital Interests** - processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

d) **Legitimate Activities** - processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the

processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

e) **Already Made Public** - processing relates to personal data which are manifestly made public by the data subject;

f) **Legal Claims** - processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity;

g) **Public Interest** - processing is necessary for reasons of substantial public interest,

h) **Preventative or Occupational Medicine** - processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services.

i) **Public Health** - processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices,

j) **Research** - processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

More detail on each lawful basis can be found on the ICO's website at: Lawful basis | ICO

Appendix 4: Data Protection Principles

Lawfulness, fairness, and transparency
Article 5(1)(a) of the GDPR says 'Personal data' shall be:

processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness, transparency').

Purpose limitation
Article 5(1)(b) says 'Personal data' shall be:

collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes.

Data minimisation
Article 5(1)(c) says 'Personal data' shall be:

adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation).

Accuracy
Article 5(1)(d) says 'Personal data' shall be:

accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy').

Storage limitation
Article 5(1)(e) says 'Personal data' shall be:

kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation').

Integrity and confidentiality (security)

Article 5(1)(e) says 'Personal data' shall be:

kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation').

Accountability

There are two key elements. Firstly, the accountability principle makes it clear that Data Controllers are responsible for complying with the GDPR. Secondly, they must be able to demonstrate their compliance.

Article 5(2) of the GDPR says:

The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 [the other data protection principles].

Further information on data protection principles can be found on the ICO's website at: A guide to the data protection principles | ICO

Appendix 5: Individuals' Rights under GDPR

1. The right to be informed

- Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR.
- Individuals must be provided with information including: our purposes for processing their personal data, our retention periods for that personal data, and who it will be shared with. This is referred to as 'privacy information'.
- Privacy information must be provided to individuals at the time we collect their personal data from them.

2. The right of access

- Individuals have the right to access their personal data.
- This is commonly referred to as subject access.
- Individuals can make a subject access request verbally or in writing.
- Organisations have one month to respond to a request.
- Organisations cannot charge a fee to deal with a request in most circumstances.

3. The right to rectification

- The GDPR includes a right for individuals to have inaccurate personal data rectified or completed if it is incomplete.
- An individual can make a request for rectification verbally or in writing.
- Organisations have one calendar month to respond to a request.
- In certain circumstances organisations can refuse a request for rectification.
- This right is closely linked to the controller's obligations under the accuracy principle of the GDPR (Article (5)(1)(d)).

4. The right to erasure

- The GDPR introduced a right for individuals to have personal data erased.
- The right to erasure is also known as 'the right to be forgotten'.
- Individuals can make a request for erasure verbally or in writing.
- Organisations have one month to respond to a request.
- The right is not absolute and only applies in certain circumstances.
- This right is not the only way in which the GDPR places an obligation on organisations to consider whether to delete personal data.

5. The right to restrict processing

- Individuals have the right to request the restriction or suppression of their personal data.
- This is not an absolute right and only applies in certain circumstances.

- When processing is restricted, organisations are permitted to store the personal data, but not use it.
- An individual can make a request for restriction verbally or in writing.
- Organisations have one calendar month to respond to a request.
- This right has close links to the right to rectification (Article 16) and the right to object (Article 21).

6. The right to data portability

- The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.
- It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.
- Doing this enables individuals to take advantage of applications and services that can use this data to find them a better deal or help them understand their spending habits.
- The right only applies to information an individual has provided to a controller.

7. The right to object

- The GDPR gives individuals the right to object to the processing of their personal data in certain circumstances.
- Individuals have an absolute right to stop their data being used for direct marketing.
- In other cases where the right to object applies, we may be able to continue processing if we can show that we have a compelling reason for doing so.
- We must tell individuals about their right to object.
- An individual can make an objection verbally or in writing.
- We have one calendar month to respond to an objection

8. Rights in relation to automated decision making and profiling.

The GDPR has provisions on:

- automated individual decision-making (making a decision solely by automated means without any human involvement); and
- profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.

The GDPR applies to all automated individual decision-making and profiling.

Further information on Individuals' Rights under GDPR is available on the ICO website at: A guide to individual rights | ICO

Appendix 6: Caldicott Principles

1. Justify the purpose(s)
Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised, and documented, with continuing uses regularly reviewed, by an appropriate guardian7.

2. Do not use personal confidential data unless it is absolutely necessary Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

3. Use the minimum necessary personal confidential data
Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

4. Access to personal confidential data should be on a strict need-to-know basis Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

5. Everyone with access to personal confidential data should be aware of their responsibilities
Action should be taken to ensure that those handling personal confidential data — both clinical and non-clinical staff — are made fully aware of their responsibilities and obligations to respect patient confidentiality.

6. Comply with the law
Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

7. The duty to share information can be as important as the duty to protect patient confidentiality
Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Further information on the Caldicott Principles can be found on the Gov.UK website: The Caldicott Principles - GOV.UK