Data Protection and Confidentiality Policy

Policy Number	IG 006
Version:	3.0
Approved by	Audit Committee
Document Author	Data Protection Officer
Date approved	15th May 2025
Next due for review	May 2028

Version control sheet

Version	Date	Policy Lead(s)	Status	Comment
1.0	May 2025	Data Protection Officer	Draft	Policy adopted from FHFT to adopt and implement at the ICB

Equality Statement

NHS Frimley aims to design and implement services, policies and measures that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others.

Throughout the development of the policies and processes cited in this document, we have:

- Given due regard to the need to eliminate discrimination, harassment and victimisation, to advance equality of opportunity, and to foster good relations between people who have shared a relevant protected characteristic (as cited under the Equality Act 2010) and those who do not share it;
- Given regard to the need to reduce inequalities between patients in access to, and outcomes from, healthcare services and in securing that services are provided in an integrated way where this might reduce health inequalities.
- Members of staff, volunteers or members of the public may request assistance with this policy if they have particular needs. If the member of staff has language difficulties and difficulty in understanding this policy, the use of an interpreter will be considered.
- We embrace the four staff pledges in the NHS Constitution. This policy is consistent with these pledges."

Contents

1 Introduction 6

2 Purpose 6

3 Scope 7

4 Definitions 7

5 Roles and Responsibilities 11

5.1 **Accountable Officer** 11

5.2 Frimley ICB Board 11

5.3 Executive Director 11

5.4 **Responsible Committee** 11

5.5 Caldicott Guardian 11

5.6 **Senior Information Risk Owner (SIRO)** 11

5.7 **Associate Director of Information Governance** 11

5.8 **Data Protection Officer**: 11

5.9 Heads of Department / Information Asset Owners (IAO) 11

5.10 Information Asset Administrators (IAA) 12

5.11 Members of staff responsibilities 12

6 The Subject Matter of the Policy 12

6.1 Regulatory Authority - Information Commissioner 12

6.2 Legal Basis for Processing Personal / Special category Data 13

6.3 Security of Processing 13

6.4 Data Protection Impact Assessments (DPIA) 13

6.5 Data Processors 14

6.6 Encryption 14

6.7 Business Continuity /Disaster Recovery Plans 14

6.8 Individuals Right 14

6.8.1 Right to be informed/transparency 14

6.8.2 Right to a copy 14

6.8.3 Right to rectification 15

6.8.4 Right to erasure (right to be forgotten) 15

6.8.5 Right to restriction of processing 15

6.8.6 Right to data portability 16

6.8.7 Right to object 16
6.8.8 Extension to managing individual right request 16
6.9 Right to Automated Decision making / Profiling 16
6.10 Right to lodge a complaint 16
6.11 Right to compensation 16
6.12 NHS Opt-out 16
6.13 Accuracy of Data 16
6.14 Consequences of a breach of the Policy 17
6.15 Offences under the Act 17
6.15.1 Unlawful obtaining of personal data 17
6.15.2 Re-identification of de-identified personal data 17
6.15.3 Alteration of personal data to prevent disclosure to a data subject 17
6.16 Reporting Loss of Personal Data 17
6.17 Contracts of Employment 18
7 Statutory Requirements 18
7.1 Caldicott Guidelines 18
7.2 NHS Confidentiality Code of Practice 19
7.3 Common Law Duty of Confidentiality 20
7.4 General Data Protection Regulation (GDPR) 20
7.5 UK Data Protection Act 2018 20
8 NHS Constitution 21
9 Dissemination//Publication 21
10 Monitoring 21
11 Review and revision 22
12 Training considerations 22
13 Stakeholder /Consultation information 22
14 References and links relating to this policy 23
15 Appendices 24
15.1 Appendix 1 – Data Protection Act 2018 Principles 24
15.2 Appendix 2 – Caldicott Principles 27
Principle 1: Justify the purpose(s) 27

Principle 2: Do not use personal confidential data unless it is absolutely necessary. 27
Principle 3: Use the minimum necessary personal confidential data. 27
Principle 4: Access to personal confidential data should be on a strict need-to-know basis. ... 27
Principle 5: Everyone with access to personal confidential data should be aware of their responsibilities. 27
Principle 6: Comply with the law. 27
Principle 7: The duty to share information can be as important as the duty to protect patient confidentiality. 27
Principle 8: Inform patients and service users about how their confidential information is used. 27

1 Introduction

To comply with the Data Protection Act 2018 ("the Act"), all information either manual or electronic which identifies a living individual must be processed (held, obtained, recorded, used and shared) in accordance with the six principles of the Data Protection Act 2018.

All NHS employees are bound by the Common Law Duty of Confidentiality, placing a legal duty on all staff working for the ICB to keep all information provided to the ICB and themselves as employees of the ICB by its stakeholders completely confidential. This legal obligation is further enforced through the codes of practice by staff's respective professions and by virtue of their contract with the ICB.

Professional bodies (e.g., NMC, GMC, CIPFA, CIMA) often release guidelines and advice for their own disciplines. These guidelines should not conflict with this policy or legislative requirements. Frimley ICB is committed to the provision of a service that is fair, accessible and meets the needs of all individuals.

2 Purpose

This Data Protection and Confidentiality Policy outlines the legal framework that governs the confidentiality of all information held by the ICB by detailing the legal obligations under the Data Protection Act 2018 which underpins the NHS Confidentiality Code of Practice 2003 which all staff must comply with.

The ICB is continually changing its processes and systems to further improve the ICB's compliance with the Data Protection Act 2018 and staff are responsible for ensuring they keep up to date with ICB policies, procedures and guidance.

Whilst working for the ICB, staff will have access to information about patients and/or about the ICB. Staff may find this information out as part of their work or see, hear or read something while on ICB premises.

All staff have a legal obligation to ensure any confidential information they come into contact with, is kept secure and confidential at all times. This duty of confidentiality relates to all information a member of staff has either created or had access to during their employment and this duty of confidentiality continues after your employment with the ICB has ceased.

Where a member of staff receives a request for information relating to an individual, staff must ensure that any disclosure of confidential information is fully justified and in compliance with the Data Protection Act 2018 or Common Law Duty of Confidentiality.

Where staff are unsure of whether to disclose the requested information or not, staff must refuse to disclose the information and seek advice from their immediate supervisor; or, if this is not possible, seek advice from, or forward the person making the request to the ICB Data Protection Officer or Caldicott Guardian or the Information Governance Department.

All staff must collect, access and/or use patient information for the purpose in which the data was collected, to provide direct care to the patient and/or assist the ICB to

meet its legal obligations.

Staff are not permitted to view or access their own records or ask another member of staff to review their records on their behalf.

3 Scope

The Data Protection Act 2018 applies to all records, both in electronic and manual formats which identifies, or could identify, an individual that are held and processed by Frimley ICB.

The Policy will apply to:

- All information used by the ICB.
- All information systems managed by or for the ICB.
- Any individual using information 'owned' by the ICB.
- Any individual requiring access to information 'owned' by the ICB.
- Any individual working on behalf of the ICB, or anyone who accesses ICB premises and information which is owned or managed by the ICB.

4 Definitions

"Processing", in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including;

- Organisation, adaptation, alteration of the information or data
- Retrieval, consultation or use of the information or data
- Disclosure of the information or data by transmission, dissemination or otherwise making available; or
- Blocking, deletion/erasure or destruction of the information or data.

The ICB advocates the method of remembering the definition of "Processing" by using the acronym HORUS – Holding, Obtaining, Recording, Using and Sharing.

Accessible Public Record - Records kept by a public body such as the ICB and covered by the Public Records Act 1958.

Anonymised Data - Data from which the identity of an individual cannot be determined. Anonymisation requires the removal of name, address, full post code and any other detail or combination or details that might support identification.

Biometric - Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or biometric data.

Caldicott Guardian - A person, usually of Director level, to oversee the arrangements for the use and sharing of person-based clinical information.

Caldicott Principles - A set of principles to control the use or flow of patient-identifiable information

CCTV - Closed Circuit Television

Code of Practice - A set of documented procedures used by public bodies to ensure they comply with legislation. For example, the NHS code of confidentiality.

Common Law - A law which is determined by decisions made by the courts and can therefore change over time. A law set by precedents.

Confidentiality - The property that information is not made available or disclosed to unauthorised individuals, entities, or processes.

Confidential Information - Confidential information could include, without limitation details of:

- Business Contacts, associates, list of suppliers and details of contract with them.
- Identities of patients
- Expenditure levels and ICB specific pricing policies
- Proposal plans or specification for the development of existing services and of new services
- Details of employees and officers of the ICB and of the remuneration and other benefits paid to them
- Presentations, tenders, projects, joint ventures, mergers, and developments contemplates, offered or undertaken by the ICB

Consent - Consent is the fact that permission has been given. A person who consents to something is, in effect, giving permission for that thing to happen.

Data - A collection of facts from which conclusions may be drawn; "statistical data".

Data Controller - This is the authority which defines the purposes for which personal data is processed. For our purposes the ICB is the data controller.

Data Processor - Any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Data Protection Act 2018 - UK wide legislation that governs the use of personal information. Its purpose is to protect the right of the individual. The Act laid down six data protection principles.

Data Protection Officer - The person within an organisation, in this case the ICB who is responsible for compliance with the Data Protection Act 2018.

Data Protection Principles - The set of standards for good practice in information processing as defined in the Data Protection Act 2018. The Act laid down six data protection principles.

Data Subject - An individual whose personal data is held by an organisation. For example, a data subject can be a patient but also a member of staff whose personal information is held by the ICB.

Destruction - Process of eliminating or deleting records, beyond any possible reconstruction.

Disclosure - The release of personally identifiable data to a third party.

DPA - Data Protection Act 2018

Explicit or Express Consent - This means the individual has articulated agreement either orally or in writing. Both terms are used to describe circumstances where a clear and voluntary preference or choice, is given. It must be given freely in circumstances where the available options and the consequences have been made clear.

Fair Processing - The first principle of the 2018 Data Protection Act is that personal data must be processed fairly and lawfully. In order to achieve this, individuals must be made aware of, and consent to, the ways in which information about them may be collected and used.

Filing system - Means any structure set of personal data which are accessible accordingly to specific criteria, whether centralised, decentralised on functional or geographical basis.

Genetic Data - Personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question

Identifiable Data - Data items that can be used to identify an individual, also referred to as personal data or personal information.

Information Sharing Protocol (ISP) - Documented rules and procedures for the disclosure and use of patient information between two or more organisations or agencies.

Information Commissioner's Office (ICO) - the UK's independent regulatory body set up to uphold information rights dealing with the Data Protection Act 2018, General Data Protection Regulation 2018, and the Freedom of Information Act 2000.

Manual Data/ Records - Information that is not processed by means of equipment.

Medical Purposes - As defined in the Data Protection Act 2018, means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

Migration / conversion - Act of moving records from one system to another, while maintaining the records' authenticity, integrity, reliability, and usability.

NHS Code of Confidentiality - A guide to required practice for those who work within or under contract to NHS organisations concerning confidentiality and patients'

consent to the use of their health records.

National Data Guardian – an independent, non-regulatory advice-giving body in England introduced by the Health and Social Care (National Data Guardian) Act 2018. This committee replaces the original Caldicott Committee.

Personal Data - Data concerning an individual. Personally identifiable data is personal data from which the identity of the individual may be deduced.

Personal Data Breach - 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.

Profiling - Means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular, to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Processing - Means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Pseudonymised Information - Means 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. The 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.

Public Interest - Exceptional circumstances that justify overruling the right of an individual to confidentiality in order to serve a broader societal interest.

Restriction of processing - The marking of stored personal data with the aim of limiting their processing in the future.

Special Category Data - Personal data consisting of a person's racial or ethnic origin, political opinions, religious beliefs or beliefs of a similar nature, membership of a trade union, physical or mental health or condition, sexual life or the commission or alleged commission of any offence (or proceedings for those offences) by that person.

Special Purposes - A term used in the Data Protection Act 2018. It refers to data used for the purposes of journalism, artistic or literary purposes.

Subject Access - This means the right of any individual (under the provisions of the 2018 Act) to have access to personal information about themselves.

5 Roles and Responsibilities

5.1 **Accountable Officer** – has ultimate accountability for the strategic and operational management of the organisation, including ensuring all policies are adhered to.

5.2 **Frimley ICB Board** – is responsible for ensuring that all policies in use in the organisation are ratified by the ICB Board.

5.3 **The Executive Director** is the Digital and Transformation who has the lead responsibility for the implementation of the policy. The Executive Director may, where appropriate, delegate responsibility for a policy to an Implementation Lead or Authorised Individual.

5.4 **The Responsible Committee** responsible for approving and oversight of compliance / monitoring of this policy is the Audit Committee.

5.5 **Caldicott Guardian** is responsible for safeguarding and governing the uses of patient information within the ICB, acting as the 'conscience' of our organisation. The Caldicott Guardian should actively support work to facilitate and enable information sharing and advice on options for lawful and ethical processing of information as required. The ICB's Caldicott Guardian is the Medical Director.

5.6 The **Senior Information Risk Owner (SIRO)** is responsible for ownership of the ICB Information Risks, to act as an advocate for information risk on the Board and provide written advice to the Accounting Officer on the content of their Statement of Internal Control in relation to information risk. The ICB's SIRO is the Director of Digital and Transformation.

5.7 **Associate Director of Information Governance** is the ICB designated Data Protection Officer. The Authorised Individual for this policy is the Associate Director of Information Governance as the ICB's designated Data Protection Officer.

5.8 **Data Protection Officer's** role includes:

- Inform and advise the ICB's awareness of the Act, including the development of policies, procedures, and guidance for individuals to support their understanding and compliance with this policy
- Monitor compliance through the auditing of staff compliance with the Act and related policies
- Ensuring staff undertake annual IG training
- Provide advice for staff when completing a Data Protection Impact Assessment
- Support the ICB's Caldicott Guardian and SIRO
- Be the point of contact for the ICO and ensure full co-operation with the ICO when required

5.9 Heads of Department / Information Asset Owners (IAO)

Data Protection procedures will vary from Department to Department. It is the responsibility of Heads of Department to ensure there are adequate and compliant procedures developed to handle personal data and sensitive personal data.

Heads of Department may delegate the day to day running of operational procedures but

may not delegate overall responsibility for the handling of personal data and sensitive personal data within their Departments.

It is the responsibility of the ICB's delegated Information Asset Owners to ensure all information assets are documented and kept appropriately secure, in line with the Data Protection Act Principles and are not kept for longer than necessary.

Information Asset Owners will be supported by Information Asset Administrators, but the overall responsibility for the management of the ICB information assets sits with the Information Asset Owners.

5.10 Information Asset Administrators (IAA)

Each computer system/database will have a designated application and/or System Manager/Information Asset Administrator. A list of these nominated personnel will be maintained as part of the Asset inventory which forms part of the ICB's Record of Processing.

The day-to-day responsibility for enforcing the Policy will be devolved to the application managers and other nominated personnel. In order to fulfil their roles, the Information Governance department will ensure regular training is provided to remind these personnel of their responsibilities and advise the most effective way of ensuring adequate information security and confidentiality.

5.11 Members of staff responsibilities

All employees of the ICB who process personal data in any form must ensure that they comply with:

- The requirements of the Data Protection Act 2018.
- The ICB's Data Protection and Confidentiality Policy, including any procedures and guidelines which may be issued from time to time.
- All staff are responsible for ensuring they complete Information Governance Training to understand the key principles of the Data Protection Act and how this applies to ICB policies, procedures and guidance.

All queries about the ICB Policy should be directed to the Information Governance Department.

6 The Subject Matter of the Policy

6.1 Regulatory Authority - Information Commissioner

Under the Data Protection Act 2018, organisations that determine the purpose for which personal data is processed (known as Data Controllers) must pay a data protection fee unless they are exempt. This is undertaken by registering with the Information Commissioners Office (ICO), therefore the ICB will continue to keep this registration up to date. Details of this registration can be found on the ICO website.

Under Article 30 of the GDPR, the ICB is required to keep a record of processing activities and will review this register on an annual basis, to ensure all processing of personal data is recorded and kept accurate and up to date.

6.2 Legal Basis for Processing Personal / Special category Data

"Processing", in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

- Organisation, adaptation, alteration of the information or data.
- Retrieval, consultation or use of the information or data.
- Disclosure of the information or data by transmission, dissemination or otherwise making available.
- Blocking, deletion/erasure or destruction of the information or data, also
- The ICB advocates the method of remembering the definition of "Processing" by using the acronym HORUS – Holding, Obtaining, Recording, Using and Sharing.
- The ICB has identified its legal basis for processing personal data under the GDPR / Data Protection Act 2018 as;

Type of data	**Patients/Customers**	**Staff**
Personal Data (Article 6)	Processing is necessary for the performance of a task carried out in the public interest or in the exercise of the official authority vested in the controller (Article 6(e)).	Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract of employment (Article 6(b)).
Special Category Data (Article 9)	We will use your information to provide preventive medicine, medical diagnosis, the provision of health care/treatment (Article 9(h)).	We will use your information for preventive or occupational medicine, for the assessment of the working capacity of the employee (Article 9(h)).

In line with Caldicott 2 recommendations, information will only be shared for the purposes of direct care with registered and regulated health care professionals who have a legitimate relationship with the patient.

6.3 Security of Processing

The Data Protection Act 2018 places an even greater emphasis on organisations to ensure that they have and implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks, some of which are detailed below and in the ICB Information Security Policies.

6.4 Data Protection Impact Assessments (DPIA)

The ICB will ensure that for all new proposed changes to the processing of personal data or special category data, a data protection impact assessment will be undertaken, and the company's Data Protection Officer (DPO) consulted to ensure that data protection principles such as data minimisation are integrated into the new processing to protect the privacy rights of data subjects.

6.5 Data Processors

Where the ICB engages with another company to undertake services, and the company will be processing the ICB's personal or special category data, the ICB will ensure that it has put in place a data processing agreement with the company/supplier. This agreement will outline the data protection responsibilities of both the ICB and the company/supplier.

6.6 Encryption

In line with the Data Protection Act 2018, the ICB will ensure that all personal data and special category are encrypted when stored on any mobile device.

6.7 Business Continuity /Disaster Recovery Plans

The ICB will ensure that it has both business continuity plans and disaster recovery plans in place for all its key/critical assets containing personal data. The ICB will ensure these plans are tested annually to maintain the integrity and availability of the information held.

6.8 Individuals Right

Under the GDPR and Data Protection Act 2018, the rights of individuals have been strengthened and are detailed below:

6.8.1 Right to be informed/transparency

All individuals have the right to be informed at the point the ICB collects information from them and within one calendar month of the ICB receiving the information from a third party company on how the ICB uses their information.

All information the ICB holds about you is managed in accordance with the Data Protection Act. For details on how we use your information please visit ICB Privacy Policy.

6.8.2 Right to a copy

Under the Data Protection Act 2018, all individuals have the right to obtain a copy of the information held about them by an organisation. Patients are able to exercise their rights by following the ICB's Individual Rights Policy.

In line with Article 15 (3) where the data subject makes a request by electronic means; unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

The ICB does not hold its documents in manual format, meaning this is the commonly used format within the ICB and will be the format in which all requested information will be provided to a data subject.

In line with Article 15 (3) the ICB is entitled to charge a reasonable fee based on administrative costs for providing further copies (first copy of information is provided free of charge). Additionally, if a request is too vague, the ICB will ask the data subject to narrow down their request, or if a data subject is requesting a very large amount of information, the ICB may charge for providing a copy.

The ICB monitors all subject access requests to ensure that they are compiled within the defined timescales in the Data Protection Act 2018.

A copy of all information held by the ICB will be provided to the requester along with:

- Details of how the ICB processes their information.
- The categories of personal data held by the ICB
- The recipients with whom their personal data will be shared, including whether any information is shared overseas
- The retention period for how long their information is held
- The individual's right to rectify, erase, restrict processing of their data
- The right to lodge a complaint to the supervisory authority
- Where the personal data was provided by a third party, who the source of the data was
- Whether any automated decision making, including profiling has been undertaken on their data

6.8.3 Right to rectification

A data subject has the right to request that their personal data is rectified without delay, and have incomplete personal data fully completed. For individuals to exercise this right, they must submit their request to the ICB.

Where the ICB has shared inaccurate data with a third party, they have a legal obligation to inform the third party of the inaccurate data shared and provide them with an accurate copy of the data subject's information.

Upon receipt of the request, the ICB will process the request within one calendar month.

6.8.4 Right to erasure (right to be forgotten)

Dependent on the legal basis for processing, a data subject may have the right to request the ICB erases their personal data where one of the following conditions applies:

- The personal data is no longer necessary in relation to the purposes from which they were collected
- The data subject objects to the processing, and there is no overriding legitimate grounds for the processing
- The personal data has been unlawfully processed

Where the ICB receives a request of this nature it will be passed to the Information Governance Department for consideration, who will provide a response to the data subject on how the ICB has processed their request.

6.8.5 Right to restriction of processing

The data subject has the right to request the ICB restricts processing their data when one of the following applies:

- Accuracy of their personal data is contested
- Processing is unlawful
- The ICB no longer needs the personal data for the purposes of processing
- Data subject has objected to the processing of their personal data pending verification on whether the legitimate grounds of the controller overrides those of the data subject

For individuals to exercise this right, they must submit their request to the Information

Governance Department. Upon receipt of the request, the ICB will process the request within one calendar month.

6.8.6 Right to data portability

The data subject has this right under the DPA 2018, dependent on an organisations legal basis, but as the ICB's legal basis for processing an individual's personal data is not reliant on the explicit consent of the data subject, this right is not applicable to the ICB processing of personal data.

6.8.7 Right to object

The data subject has this right to object to how the ICB is processing their data. For individuals to exercise this right, they must submit their request to the Information Governance Department. Upon receipt of the request, the ICB will process the request within one calendar month,

6.8.8 Extension to managing individual right request

Where an individuals request is excessive, and the ICB requires more time; the data subject will be informed the ICB requires a further time to process their request, up to a maximum of another 2 months.

6.9 Right to Automated Decision making / Profiling

The data subject has the right not to be subjected to a decision based solely on automated processing, including profiling. As the ICB does not undertake any automated decision making or profiling, this right is not applicable.

6.10 Right to lodge a complaint

The ICB recognises an individual's right to lodge a complaint with the ICO. This information has been placed on the ICB website as well as being communicated to patients when they choose to exercise their rights under the Data Protection Act 2018.

6.11 Right to compensation

The ICB recognises the rights of individuals to seek compensation where they have suffered damage/distress as a breach of the Data Protection Act 2018.

6.12 NHS Opt-out

The ICB acknowledges the review undertaken in 2016 by the NHS and Social Care National Data Guardian. The review not only agreed the NHS and Social Care need to process patient information on a wider scale to help improve the care and treatment delivered, but also agreed there were circumstances when patients can choose to opt out with how the NHS uses their information. Details of the national opt out in the NHS can be found at:
https://www.gov.uk/government/publications/review-of-data-security-consent-and- opt-outs

The ICB will ensure where patients have exercised their rights to opt out of their information being used to secondary purposes, this will be recorded on the ICB's system and respected.

6.13 Accuracy of Data

All staff are responsible for:

- Checking any patient, staff or other individual's information they access is accurate and up to date.
- Correcting any inaccurate data. This may only be undertaken if the member of staff has sufficient rights to amend data. Otherwise staff must bring the discrepancy to the attention of the system administrator or line manager.
- Checking any personal information they provide to the ICB in connection with their employment is accurate and up to date, e.g., change of address. The ICB cannot be held responsible for any errors unless the member of staff has informed the ICB.

6.14 Consequences of a breach of the Policy

Breaches of this Policy will be considered a serious disciplinary matter and will be dealt with accordingly. Examples of offences which may be considered to be gross misconduct (the list is not exhaustive) which may result in immediate dismissal are:

- Offences as detailed in the Data Protection Act 2018 (see section 5.12)
- Unlawful disclosure of Personal Data and/or Sensitive Personal Data
- Inappropriate use of Personal Data and/or Sensitive Personal Data.
- Misuse of Personal Data and/or Sensitive Personal Data which results in any claim being made against the ICB.
- Loss of Personal Data and/or Sensitive Personal Data.
- Unauthorised disclosure or copying of information belonging to the ICB

6.15 Offences under the Act

The Data Protection Act 2018 further adds to the offences in the Data Protection Act 1998, which are:

6.15.1 Unlawful obtaining of personal data

It is an offence for an individual to knowingly or recklessly:

- obtain or disclose personal data without the consent of the data controller
- procure the disclosure of persona data to another individual without the consent of the data controller
- after obtaining personal data, to retain it without the consent of the individual who was the controller in relation to the personal data when it was obtained

6.15.2 Re-identification of de-identified personal data

It is an offence for an individual knowingly or recklessly to re-identify information that is de-identified personal data without the consent of the data controller responsible for de-identifying the personal data.

6.15.3 Alteration of personal data to prevent disclosure to a data subject

It is an offence for an individual to alter, deface, block erase, destroy or conceal information with the intention of preventing disclosure of all or part of the information that the persona making the request would have been entitled to receive.

6.16 Reporting Loss of Personal Data

Any breaches/losses of personal data must be reported using the ICB's Incident reporting process. In line with Article 33 of the GDPR, the ICB must report any breaches of personal data within 72 hours to the ICO with the following information:

- Nature of the personal breach.

- Categories and approximate number of data subject concerned.
- Name and contact details of the Data Protection Officer.
- Likely consequences of the personal breach.
- Measures taken or proposed to be taken to address the personal breach.

Additionally, where the personal data breach is likely to result in a high risk to the rights and freedoms of an individual, the ICB will communicate the personal data breach to the individual without undue delay with the following information and an apology:

- Name and contact details of the Data Protection Officer.
- Likely consequences of the personal breach.
- Measures taken or proposed to be taken to address the personal breach.

NHS Digital is updating the guidance on how the NHS organisations report their data losses. The ICB will continue to follow the NHS digital guidance for reporting its personal data incidents.

6.17 Contracts of Employment

Staff contracts of employment are produced and monitored by the ICB's People Department. All contracts of employment include an information governance/data protection and confidentiality clause. Agency and contract staff are subject to the same rules.

The ICB has a Confidentiality Agreement that non- ICB staff must sign before undertaking any work in or on behalf of the ICB.

7 Statutory Requirements

7.1 Caldicott Guidelines

In 1997 the Caldicott Committee Report found that confidentiality and security compliance was patchy across the NHS. In response to this patchy compliance across the NHS, the Caldicott Committee developed 6 principles which staff must apply when using patient information. In 2013, a seventh principle was introduced. In 2020, as part of the National Data Guardian review, the principles were amended to include an eighth principle:

1. Justify the purpose(s).
2. Do not use personal confidential data, unless it is absolutely necessary.
3. Use the minimum necessary personal confidential data.
4. Access to person confidential data should be on a strict need-to-know basis.
5. Everyone with access to personal confidential data should be aware of their responsibility.
6. Comply with the law.
7. The duty to share information can be as important as the duty to protect patient confidentiality.
8. Inform patient and service users about how their confidential information is used.

A detailed explanation of the 8 Caldicott principles can be found at Appendix A.

7.2 NHS Confidentiality Code of Practice

The Department of Health Confidentiality Code of Practice published in 2003 states its implementation will enable an NHS organisation to achieve a confidential service in which all patient information is processed fairly, lawfully and as transparently as possible.

The Department of Health Confidential model has 4 main elements:

PROTECT – look after patient's information. In order to provide a confidential service, the ICB needs to ensure it protects patient information at all times, so only staff who have a need to access the confidential information can do so.

Staff should share the minimum information necessary to support patient safe care or to satisfy other legitimate purposes, bearing in mind missing information could cause harm patient care.

A patient's confidentiality must be respected in response to enquiries from external individuals or organisations (e.g., media, police, and insurance companies). In these circumstances express consent must be obtained from the patient and/or proper (legal) authority demonstrated before any disclosure is made.

Staff must not use any of the ICB IT systems to make an unauthorised disclosure or copy of confidential information belonging to the ICB.

INFORM – ensure that patients are aware of how their information is used
The ICB must inform patients of the intended use of their information, giving them the choice to give or withhold their consent and protect their identifiable information from unwarranted disclosure.

PROVIDE CHOICE – allow patients to decide whether their information can be disclosed or used in particular ways.
Patients have different needs and values – this must be reflected in the way they are treated, both in terms of their medical condition and the handling of their personal information.

Staff must:
Seek the patient's consent prior to using their information in ways that do not directly contribute or support the delivery of their care.
Respect a patient's decisions to restrict the disclosure or use of their information, other than where exceptional circumstances apply.
Communicate effectively with patients to ensure they understand the implications if they choose to agree or restrict the disclosure of their information.

IMPROVE – always look for better ways to protect, inform and provide choice
The ICB accepts that technology changes, therefore the ICB will continually review its processes to ensure the 4 elements of the Department of Health Confidentiality Code of Practice is protecting patient information to the highest level at all times.

7.3 Common Law Duty of Confidentiality

A duty of confidentiality arises when one person discloses information to another (e.g., patient to clinician) in circumstances where it is reasonable to expect that the information will be held in confidence. This is a legal obligation that is derived from case law, built up over many years.

This Common Law Duty of Confidentiality places an obligation on all individuals working in and for the ICB to ensure that all confidential information which they come into contact with is kept securely and remains confidential.

Whilst the Data Protection Act 2018 only covers living individuals' information, the Common Law Duty of Confidentiality ensures a patient's right to confidentiality continues after their death.

7.4 General Data Protection Regulation (GDPR)

GDPR adds in new concepts of Accountability and Demonstrability for the processing of personal data on organisations, as well as increasing the rights of an individual to how organisations process their personal data.

7.5 UK Data Protection Act 2018

The Data Protection Act 1998 has been repealed by the Data Protection Act 2018, and mirrors the GDPR and will remain in force, as GDPR no longer applies since the UK exited the EU. The purpose of the Act is to enhance, protect the rights and privacy of individuals, and to ensure that data about them cannot be processed without their knowledge or consent wherever possible. The Act covers personal data relating to living individuals.

The Act stipulates that any organisation processing personal data must comply with 6 principles of good practice. The legally enforceable principles are:

1. Processing of personal data must be lawful and fair,
2. Processing of personal data must be specified, explicit and legitimate and not processed in a manner which is incompatible with the purpose for which it was collected,
3. Processing of personal data must be adequate, relevant, and not excessive,
4. Processing must be accurate and kept up to date,
5. Processing must not be kept for no longer than necessary for the purpose for which it is processed,
6. Processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures.

An explanation of the 6 Data Protection Act Principles can be found in Appendix A.

Bribery Act 2010 – the ICB has a responsibility to ensure that all staff are made aware of their duties and responsibilities arising from The Bribery Act 2010. The Bribery Act 2010 makes it a criminal offence to bribe or be bribed by another person by offering or requesting a financial or other advantage as a

reward or incentive to perform a relevant function or activity improperly performed. The penalties for any breaches of the Act are potentially severe. There is no upper limit on the level of fines that can be imposed and an individual convicted of an offence can face a prison sentence of up to 10 years.

For further information see http://www.justice.gov.uk/guidance/docs/bribery-act2010-quick-start-guide.pdf.

Due consideration has been given to the Bribery Act 2010 in the review of this policy and no specific risks were identified.

8 NHS Constitution

The ICB is committed to:

Designing and implementing services, policies and measures that meet the diverse needs of its population and workforce, ensuring that no individual or group is disadvantaged.

This Policy supports the NHS Constitution as follows:

The NHS aspires to the highest standards of excellence and professionalism in the provision of high-quality care that is safe, effective and focused on patient experience; in the planning and delivery of the clinical and other services it provides; in the people it employs and the education, training and development they receive; in the leadership and management of its organisations; and through its commitment to innovation and to the promotion and conduct of research to improve the current and future health and care of the population.

9 Dissemination//Publication

As part of the induction process, both corporate and departmental, all ICB employees will be made aware of their responsibilities in connection with the Acts mentioned in this Policy. This will be provided through their Statement of Terms and Conditions and the completion of national information governance training and any specialist training identified as applicable to their role.

10 Monitoring

The ICB will monitor staff compliance against this policy through the monitoring of reported ICB incidents, audits of staff working practices relating to breaches of confidentiality, loss of personal information.

Criteria	Measurable	Frequency	Reporting to	Action Plan/Monitoring
Audit	Yes	Annual	DPO	To audit staff working practices
Data Mapping	Yes	Annual	DPO	Document all data flows in department
System Assurance	Yes	New System or any upgrade	DPO	Assure security of any electronic asset in use in the ICB

Criteria	Measurable	Frequency	Reporting to	Action Plan/Monitoring
Incident	Yes	Ad hoc	DPO	Review of ICB policies/processes
Survey	Yes	Annual	DPO	Survey of staffing knowledge and understanding of IG related policy

11 Review and revision

This policy will be reviewed every three years by the Document Author to ensure continued validity and relevance, with a schedule of proposed amendments presented to the Audit Committee for approval.

12 Training considerations

Staff will be required to complete the applicable IG related training applicable to their role, which is recorded on the ICB IG training register. The IG Department monitors staff compliance with the required training and reported ICB staff compliance to the Audit Committee.

13 Stakeholder /Consultation information

The document author has responsibility to ensure consultation takes place with the appropriate stakeholders.

The draft document should be circulated to the identified stakeholders clearly identifying the deadline for responding and the named contact for comments to be forwarded to.

14 References and links relating to this policy

- *Data Protection Act 2018, c. 12*. Available at: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

- General Data Protection Regulations (GDPR) (2016), *Official Journal of the European Union* L 119, pp. 1-88. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

- Department of Health (2003) *NHS confidentiality code of practice*. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/200146/Confidentiality_-_NHS_Code_of_Practice.pdf.

- National Data Guardian for Health and Social Care (2020) *The eight Caldicott principles*. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/942217/Eight_Caldicott_Principles_08.12.20.pdf.

- NHS Digital (2022) *NHS and social care data: off-shoring and the use of public cloud services: guidance*. Available at: https://digital.nhs.uk/data-and- information/looking-after-information/data-security-and-information- governance/nhs-and-social-care-data-off-shoring-and-the-use-of-public-cloud- services/guidance.

15 Appendices

15.1 Appendix 1 – Data Protection Act 2018 Principles

There are six principles of good practice within the Data Protection Act 2018. These are normally referred to as the 'data protection principles'.

Principle 1 – "Personal data shall be processed fairly, lawfully and in a transparent manner"

Fair Processing

There is a requirement to make the general public, who may use the services of the ICB, aware of why the ICB needs information about them, how this is used and to whom it may be disclosed.

This requires the ICB to make sure individual understand how their information is to be used to support their healthcare and that they have no objections.

Where staff are not able to answer a patient's queries on how their information is used, they should be referred to either the ICB's Information Governance Department.

Transparent

The ICB needs to make it transparent to individuals how their information is being used. For details on how the ICB's use personal data, individuals can visit ICB Privacy Policy.

Principle 2 - "Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner which is incompatible with those purposes"

All databases which hold and/or process personal information about living individuals must be registered with the ICB Information Governance department, which will inform the ICB's Record of Processing activities.

For the purposes of Data Protection, a database is considered to be any collection of personal information (more than 51 records) that can be processed by automated means, e.g.,

- Patient records (names and addresses etc.) for appointments
- Patient details used for prescribing drugs
- Patient information used for research, e.g., where only NHS number (or other personal identifier may be allocated) and clinical details may be held – this could be a spreadsheet or Access database
- Staff records held on Excel to monitor annual leave and sickness
- When collecting personal information, it is essential that the data subject is clear about why the information is being collected and what the information is to be used for. The same information can be used for several different purposes as long as the data subject has been made aware of all of these purposes.

Principle 3 – "Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed".

Information collected from individuals should be complete and should all be justified as being required for the purpose for which they are being requested. Information must not be collected because it might be useful at a future date.

Principle 4 – "Personal data shall be accurate and, where necessary, kept up to date"
The ICB has to ensure that all information held on any media is accurate and up to date. The accuracy of the information can be achieved by implementing validation routines, some of which will be system specific, and details must be provided of these validation processes to the system/information users.

Users of software will be responsible for the quality (i.e., Accuracy, Timeliness, Completeness) of the data held in their software/systems and must carry out quality assurance audits.

Staff information should also be checked for accuracy on a regular basis – either by the manager or by the HR/Personnel department.

There may be instances when non-current information needs to be retained, e.g., for audit purposes or historical research, where this is the case, the information must be correct at the time it was recorded.

Principle 5 – "Personal data kept for no longer than is necessary for the purposes for which the personal data are processed"
All records containing personal information must only be stored for the appropriate length of time. The "DH Records Management: NHS Code of Practice" provides comprehensive guidance for NHS organisations on the retention period for all NHS records. Further details of how this affects the ICB, and actions required to comply with it, are detailed in the ICB's Records Management Policies.

If the information on the computer or manual record is not the main record, this is considered to be transient data. The ICB will develop procedures/ guidance for staff to know and understand what information should be culled, archived or destroyed when no longer deemed to be of use.

The ICB has a legal obligation to maintain confidentiality standards for all information relating to patients, employees, and ICB business. It is important that this information is disposed of in a secure manner.

Principle 6 – "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

All information relating to identifiable individuals must be kept secure at all times. The ICB will implement policies/procedures to protect ICB information against unauthorised processing of information, accidental loss, destruction and damage to this information. Measures being undertaken are:

- All removal media will be encrypted
- All laptops will be encrypted.
- All software and data are removed from redundant hardware and media storage (e.g., tapes, disks) before the hardware is removed from the ICB.
- Confidential paper waste is shredded or is collected and held in a secure area prior to shredding/incinerating.
- Staff will not share usernames and passwords.
- ICB will implement systems that have appropriate security measures and functionality.
- Information Asset Administrator

Each Information Asset Administrator is responsible for ensuring that the system they manage complies with the Data Protection Act. This responsibility includes keeping the system security policy up to date and ensuring procedures are in place to achieve a high level of data security and quality.

Each Information Asset Administrator is responsible for ensuring:

- users are set up on the system on a need to know basis
- unusual requests for disclosure are scrutinised
- staff are aware of their responsibilities regarding security, data protection and confidentiality issues
- Back-ups
- Each Information Asset Administrator is responsible for ensuring the system they are responsible for is regularly backed up.

Some of the ICB IT Systems will have their systems backed up on a daily basis by the CSU IT Department. The master copy of programs and back-ups of data will be kept securely by the CSU IT departments.

Disclosure of information/information in transit
Information about identifiable individuals (such as patients and staff) must only be disclosed on a strict need to know basis. Strict controls governing the disclosure of patient identifiable information is also a requirement of the Caldicott recommendations. However, some disclosures of information may occur because there is a statutory requirement upon the ICB to disclose, e.g., Court Order; other legislation requires disclosure, e.g., tax office, pension agency - for staff; notifiable diseases - for patients.

Only ICB approved transport couriers should be used at all times. Packaging should be sufficient to protect the contents from any physical damage during transit and in accordance with manufacturer's specifications.

Contracts
Contracts between the ICB and third parties should include the ICB standard confidentiality clause, which should be disseminated to the third party's employees.

15.2 Appendix 2 – Caldicott Principles

Principle 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 the appropriate guardian.

Principle 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).

Principle 3: Use the minimum necessary personal confidential data.

Where the 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.

Principle 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.

Principle 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 responsibility and obligations to respect patient confidentiality.

Principle 6: Comply with the law.

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

Principle 7: The duty to share information can be as important as the duty to protect patient confidentiality.

Health and Social care professional should have the confidence to share information in the best interest 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.

Principle 8: Inform patients and service users about how their confidential information is used.

A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant, and appropriate information – in some cases, greater engagement will be required.