



**Nottingham and
Nottinghamshire**
Integrated Care Board

Confidentiality and Data Protection Policy

June 2025 – June 2028

CONTROL RECORD	
Title	Confidentiality and Data Protection Policy
Reference Number	IG-002
Version	4.2
Status	Final
Author	Information Governance Delivery Manager
Sponsor	Director of Corporate Affairs
Team	Information Governance
Amendments	Section 6 – Artificial Intelligence added/updated to set requirements for lawful, ethical, and secure use of AI, including data protection and staff responsibilities.
Purpose	This Data Protection Policy aims to detail how the ICB meets its legal obligations and NHS requirements concerning confidentiality and Data Protection standards.
Superseded Documents	Confidentiality and Data Protection Policy v4.1
Audience	All employees of the ICB (including all individuals working in a temporary capacity, including agency staff, seconded staff, students and trainees, and any self-employed consultants or other individuals working for the ICB under contract for services).
Consulted with	SIRO, Caldicott Guardian and Data Protection Officer
Equality Impact Assessment	Complete – see section 12
Approving Body	v4.2 (minor amendments) approved by IG Steering Group
Date approved	November 2025
Date of Issue	November 2025
Review Date	June 2028
<p>This is a controlled document and whilst this policy may be printed, the electronic version available on the ICB’s document management system is the only true copy. As a controlled document, this document should not be saved onto local or network drives.</p>	

NHS Nottingham and Nottinghamshire Integrated Care Board (ICB)’s policies can be made available on request in a range of languages, large print, Braille, audio, electronic and other accessible formats from the Engagement and Communications Team at nnicb-nn.comms@nhs.net.

Contents

1	Introduction	Page 4
2	Purpose	Page 5
3	Scope	Page 5
4	Roles and Responsibilities	Page 5
5	Definitions	Page 7
6	Process	Page 9
	• Legislation	Page 9
	• NHS Related Guidance	Page 10
	• Overview of the General Data Protection Regulation and the Data Protection Act 2018	Page 10
	• Data Protection Principles	Page 11
	• Individual Rights	Page 12
	• Determining Personal Data	Page 12
	• Common Law Duty of Confidentiality	Page 14
	• Consent	Page 14
	• Caldicott and the National Data Guardian	Page 15
	• Caldicott Principles	Page 16
	• Disclosure of Personal Confidential Data	Page 16
	• Keeping Individuals Informed	Page 17
	• Data Protection Contractual Clauses	Page 17
	• Data Protection Impact Assessments	Page 18
	• Artificial Intelligence	Page 18
7	Equality and Diversity Statement	Page 19
8	Communication, Monitoring and Review	Page 20
9	Staff Training	Page 20
10	Interaction with other Policies	Page 21
11	References	Page 21
12	Equality Impact Assessment	Page 23
	Appendix A: Overview of Legislation	Page 28
	Appendix B: Overview of NHS Guidance	Page 30

1. Introduction

- 1.1 This policy applies to the NHS Nottingham and Nottinghamshire Integrated Care Board, hereafter referred to as 'the ICB'.
- 1.2 The ICB has a legal obligation to comply with all appropriate legislation in respect of data, information and information security. It also has a duty to comply with guidance issued by the Department of Health and Social Care (DHSC); the Information Commissioner (ICO); other advisory groups to the NHS; and guidance issued by professional bodies.
- 1.3 Information in all its forms is crucial to the effective functioning and good governance of the ICB which is committed to efficient and effective information management and information security to ensure that all information and information systems, on which the ICB depends, are adequately protected. Information, paper and electronic systems, applications and the networks that support the ICB are important organisational assets.
- 1.4 All legislation and NHS statutory requirements relevant to an individual's right of confidence and the ways in which that can be achieved and maintained are paramount to the ICB. These requirements are covered in ICB policies, and any breaches of policy and/ or information legislation and regulations could result in reputational damage and penalties being imposed upon the ICB and/ or its employees for non-compliance.
- 1.5 This policy applies to all information/ data, personal and special category (sensitive personal) processed by the ICB pursuant to its operational duties and activities, regardless of whether it is processed in electronic or in paper (hard copy) form, any communications sent to or from the ICB and any ICB information/ data held on systems external to the ICB's network.
- 1.6 The ICB collects and processes personal data about people with whom it interacts with to carry out its business functions and provide its services. Such people include but are not limited to patients, the public employees (present, past and prospective), suppliers and other business contacts. The data may include identifiers such as name, address, email address, data of birth, NHS Number, National Insurance Number. It may also include private and confidential information, and special categories of personal data.
- 1.7 The ICB and its employees have a responsibility to protect information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction.
- 1.8 This policy has been reviewed in relation to having due regard to the Public Sector Equality Duty (PSED) of the Equality Act 2010 to eliminate discrimination, harassment, victimisation; to advance equality of opportunity; and foster good relations.

2. Purpose

- 2.1 This Confidentiality and Data Protection Policy aims to detail how the ICB meets its legal obligations and NHS requirements concerning confidentiality and data protection requirements. These requirements are primarily based upon key pieces of legislation, the UK Data Protection Act 2018 and the UK General Data Protection Regulation, Privacy and Electronic Communications Regulation (PECR), Network and Information Systems (NIS); however, other relevant legislation and appropriate guidance will be referenced.

The ICB must also meet the requirements of the Common Law Duty of Confidentiality (CLDC) to enable the lawful processing of personal confidential data.

3. Scope

- 3.1 All individuals employed by the ICB including all individuals working in a temporary capacity, including agency staff, seconded staff, students and trainees, and any self-employed consultants or other individuals working for the ICB under contract for services, including Governing Body and lay members hereinafter referred to as 'employees' must adhere to this policy. Third Parties will be governed by any associated information sharing or processing agreements and will be made aware of this policy.

4. Roles and Responsibilities

- 4.1 The ICB has a legal duty to comply with all relevant information legislation and regulations including the Common Law Duty of Confidentiality.

Roles	Responsibilities
Chief Executive	The Chief Executive is responsible for ensuring that the responsibility for data protection is allocated appropriately within the ICB and that the role is supported.
Integrated Care Board	The ICB is responsible for the implementation of this policy and for ensuring that: <ul style="list-style-type: none">• All employees and individuals as set out in the scope of this document, when dealing with personal confidential data are aware of the need for compliance with information legislation and regulation including associated provisions.• There is a Senior Health Professional appointed as Caldicott Guardian to oversee the processing of personal confidential data.

Roles	Responsibilities
	<ul style="list-style-type: none"> • All staff are also aware of the requirements of the Common Law Duty of Confidentiality as set out in the DHSC Confidentiality: NHS Code of Practice 2003 and the HSCIC/ NHS Digital Guide to Confidentiality 2013. • There is a Senior Information Risk Owner (SIRO): an executive appointed to take ownership of information and information security risk. • The ICB Board is aware of the detailed provisions of information legislation and regulation and any subsequent guidance issued by the Department of Health and Social Care and by the Information Commissioner's Office. This takes place through updates from the Audit and Risk Committee and directly from the Information Governance Steering Group, Data Protection Officer and Associate Director of Corporate Affairs as appropriate. • The processing of personal data within the ICB is compliant with information legislation and relevant and applicable regulations. • Registration with the Information Commissioner's Office is kept up to date through annual renewals by the Head of Information Governance. • There is an appointed Data Protection Officer appointed and their details and contact information is publicised on the ICB website.
Caldicott Guardian	The Caldicott Guardian will be responsible for ensuring that confidential information about health and social care service users is used ethically, legally, and appropriately.
Data Protection Officer (DPO)	The DPO is responsible for overseeing data protection legislation strategy and implementation to ensure compliance with requirements and to advise the ICB on its data protection obligations.
Senior Information Risk Owner (SIRO)	The Senior Information Risk Owner (SIRO) has organisational responsibility for all aspects of information risk including those relating to confidentiality and data protection compliance.
Information Asset Owners	Information Asset Owners are responsible for understanding and addressing risks relevant to the "information assets" within their areas of responsibility. They must ensure that the policy and its supporting standards and guidelines are built

Roles	Responsibilities
	into their local processes and their teams are aware of these compliance requirements.
All Managers	All managers are responsible for ensuring that their staff receive relevant training, guidance and support to understand and adhere to this policy and all appropriate supporting guidance and local processes.
All Employees	All staff must adhere to the ICB's policies, procedures and local processes relating to the processing of personal information. All staff members are responsible for maintaining compliance with the Data Protection legislation and for reporting non-compliance through the ICB's incident reporting process.

5. Definitions

Term	Definition
Consent as defined under GDPR	Any freely given specific and informed indication of [the data subject's] wishes by which the data subject signifies [his/ her] agreement to personal data relating to [him/ her] being processed'.
(Data) Controller	Means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
(Data) Processor	Means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Secondary Use Purposes (indirect care)	<p>Purposes other than direct or 'primary' clinical care, e.g.,</p> <ul style="list-style-type: none"> • Healthcare planning. • Commissioning of services. • National Tariff reimbursement. • Development of national policy. <p>Activities that contribute to the overall provision of services to a population as a whole or a group of patients with a particular condition. It also covers health services management, preventative medicine, and medical research.</p>

Term	Definition
Sub-processor	A sub-processor is a third party data processor engaged by a data processor who has or will have access to or process personal data from a Data Controller .
Data Subject or Natural Person	The identified or identifiable living individual to whom personal data relates.
Personal Confidential Data	This is personal information about identified or identifiable individuals which is also confidential. 'Personal' includes the Data Protection Act definition of personal data, but it can also include the deceased as well as the living. 'Confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence' e.g., health records. It is adapted to include 'special categories' data as defined in the Data Protection Act.
Personal Data	Any information relating to a person (a 'data subject') who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.
Pseudonymised Information	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.
Special Category Data	<p>Personal data revealing racial or ethnic origin, personal data revealing political opinions, personal data revealing religious or philosophical beliefs, personal data revealing trade union membership, genetic data, biometric data (where used for identification purposes), data concerning health, data concerning a person's sex life, and data concerning a person's sexual orientation.</p> <p>This does not include personal data about criminal allegations, proceedings or convictions, as separate rules apply.</p>
Right of Access (Living individuals)	The right of access, commonly referred to as subject access, gives individuals the right to obtain a copy of their personal data, as well as other supplementary information. It helps

Term	Definition
	individuals to understand how and why the ICB is using their data, and that it is lawful.
Right of Access (Deceased individuals)	<p>The Access to Health Records Act 1990 grants rights to certain individuals to see records about a deceased patient in a hospital and other health records. This only applies to records made on or after 1 November 1991. Access is available to:</p> <ul style="list-style-type: none"> • The patient’s personal representative (this will be the executor of the will or the administrator of the estate). • Any person who may have a claim arising out of the patient’s death.
Individual Rights	<ul style="list-style-type: none"> • The right to be informed. • The right to rectification. • The right of access. • The right to be forgotten (erasure). • The right to restrict the processing of your data. • The right to data portability. • The right to object. • Rights regarding automated profiling and decision making. <p>https://ico.org.uk/for-organisations/accountability-framework/individuals-rights/</p>

6. Process

Legislation

6.1 The legislation listed below also refers to issues of security and confidentiality of personal data (for a more detailed description, see **Appendix A**):

- Access to Health Records Act 1990
- Access to Medical Reports Act 1988
- UK Data Protection Act 2018
- Computer Misuse Act 1990
- Crime and Disorder Act 1998
- Freedom of Information Act 2000
- Health and Care Act 2022
- Human Rights Act 1998

- Privacy and Electronic Communications Regulations 2003
- Investigatory Powers Act 2016
- UK General Data Protection Regulation (UK GDPR)
- Common Law Duty of Confidentiality (case law)
- The Health & Social Care (National Data Guardian Act) 2018

NHS and Related Guidance

6.2 The following are the main publications referring to security and confidentiality of personal confidential data:

- Caldicott Review 2013 and 2020
- Caldicott Principles 2020
- Employee Code of Practice (Information Commissioner's Office)
- HSCIC (then NHS Digital now NHS England): Guide to Confidentiality 2013
- ISO/ IEC 27001:2005 and 17799:2005 Information Security Standard
- NHS Constitution 2021
- Records Management Code of Practice 2021
- Data Sharing Code of Practice (Information Commissioner's Office)
- Subject Access Code of Practice (Information Commissioner's Office)
- Anonymisation - Managing Data Protection Risk (Information Commissioner's Office)
- National Data Guardian - Data Security Standards

Further guidance can also be found via Data Security & Protection Toolkit
<https://www.dsptoolkit.nhs.uk/>

Overview of the General Data Protection Regulation (GDPR) and the Data Protection Act (DPA) 2018

6.3 Data protection legislation sets out specific rights for individuals and affirms that organisations must proactively assure themselves as to processing of the personal data they hold. They must ensure that there is a legal basis for the processing. Where new uses or processes for information are introduced, these must be subject to a Data Protection Impact Assessment (DPIA), and in certain circumstances approval must be obtained from the Information Commissioner's Office before that processing may commence.

- 6.4 Data protection legislation applies to all personal data held in manual/ paper files, computer databases, videos, and other automated media, about living individuals. Personal data should only be disclosed when it is fair and lawful to do so. Any unauthorised disclosure of personal data by an employee may result in disciplinary action or criminal prosecution.
- 6.5 The ICB must be registered with the Information Commissioner's Office and the registration is maintained by the ICB Information Governance Team. A fee is paid as part of this registration process.
- 6.6 Under a provision of data protection legislation an individual can request access to their personal data (Subject Access Request) regardless of the media in which this information may be held/ retained. The ICB has an Information Rights Procedure which sets out how the ICB upholds all individual's rights under data protection, including dealing with Subject Access Requests.
- 6.7 Please see **Appendix B** for an overview of NHS and related guidance.

Data Protection Principles

- 6.8 Article 5(1) of the GDPR lists the data protection principles. It requires that data controllers ensure personal data shall be:
 - (a) Processed lawfully, fairly and in a transparent manner in relation to individuals.
 - (b) 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 not be considered to be incompatible with the initial purposes.
 - (c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
 - (d) 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.
 - (e) 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 subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

- (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.

Article 5(2) requires that:

“The controller shall be responsible for, and be able to demonstrate, compliance with the principles.”

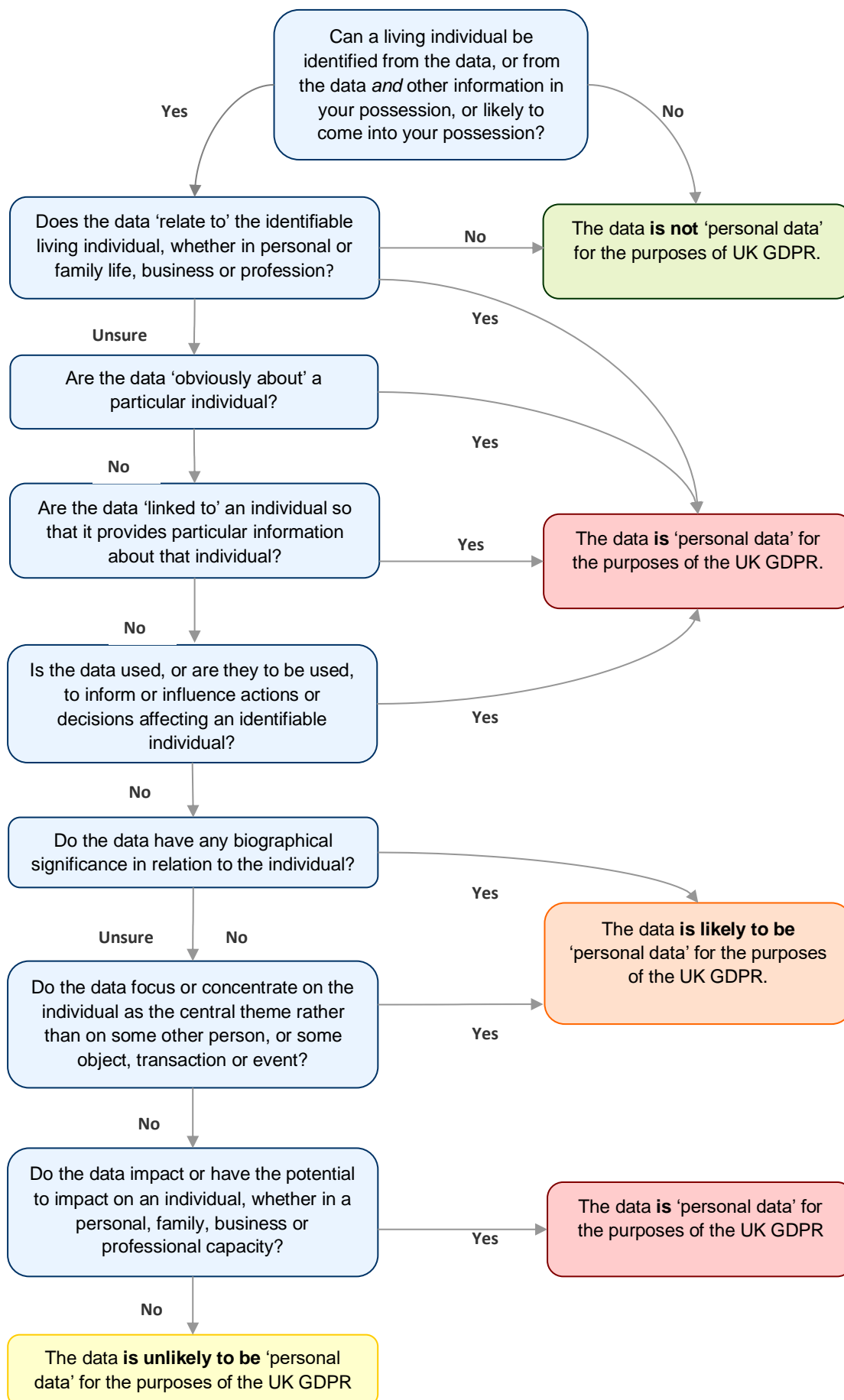
Individual Rights

6.9 Data rights for individuals are:

- The right to be informed.
- The right to rectification.
- The right of access.
- The right to be forgotten (erasure).
- The right to restrict the processing of your data.
- The right to data portability.
- The right to object.
- Rights regarding automated profiling and decision making.

Determining Personal Data

6.10 The following flow chart can be used by staff to help assess when certain kinds of data may or may not constitute Personal Data:



Common Law Duty of Confidentiality (CLDC)

- 6.11 All NHS Bodies and those carrying out functions on behalf of the NHS have a duty of confidence to service users and a duty to support professional and ethical standards of confidentiality. A duty of confidence arises when a person discloses information to another (e.g., patient to clinician or employee to employer) in circumstances where it is reasonable to expect that the information will be held in confidence. It is a legal obligation derived from case law and a requirement established in professional codes of conduct that the information is kept confidential and used in a way that would be expected by those imparting the information.
- 6.12 In summary, information cannot be disclosed further unless one or more of the following applies:
- A mandatory legal requirement or power that enables the CLDC to be set aside, such as The Children Act 1989 which requires information to be shared in safeguarding cases
 - A Court Order where a judge has ordered that specific and relevant information is provided, and to whom
 - An overriding public interest where it is judged that the benefit of providing the information outweighs the rights to privacy for the patient concerned and the public good of maintaining trust in the confidentiality of the service
 - Legal support for the use of the data without consent under the Health Services (Control of Patient Information) Regulations 2002, under section 251 of the NHS Act 2006; or
 - Explicit or implied consent.

Consent

- 6.13 Consent is one of several legal bases for processing personal data under Data Protection law. Where explicit consent is the most appropriate legal basis for processing it should be formally recorded. Where explicit consent is relied upon it must be:
- Fully informed
 - Freely given
 - Specific to the circumstances, *and*
 - With positive indication from the Subject

In most cases, those consenting *must* be able to withdraw their consent at any feasible point and must be given information at the time of consenting on how

they are able to do so. Exceptions for this are where an individual has consented to a one-off activity that cannot be undone. This does not exempt an individual from requesting exercise of other rights however such as right to request personal data is deleted. Such instances are considered on case by case basis.

6.14 Under the Common Law Duty of Confidence, which differs slightly from the consent described in the GDPR:

- **Implied consent** will normally apply where data is being used and there is a reasonable expectation of the Subject or their representative, that their data would need to be used in that way, to carry out a mutually agreed or understood activity. For example, when a clinician refers a patient to another clinician as part of care of which the patient is already aware, and this is also explained to the patient. The patient does not object and so consent is implied.

This type of consent will not usually be applicable to the purposes for which the ICB is processing personal data because it is not involved in direct patient care and processes minimal patient data.

- **Explicit consent** applies where an individual has agreed to the use of data for a specified purpose, after they have been fully informed. Consent under CLDC does not need to meet the requirements for consent set out in the GDPR.

6.15 Wherever the processing of data relies on consent either under GDPR or common law, it must be recorded by the staff obtaining it, in the appropriate place whether on an individual's record, file, complaint account, etc. Consent is also captured as applicable (where processing relies on it) on the ICB's data flow mapping register.

6.16 Consent must be reviewed and refreshed where the nature, scope or purpose of the data processing changes, where processing continues over an extended period of time, or where children have reached the age of adulthood and can provide consent for themselves.

Caldicott and National Data Guardian

6.17 The Caldicott Report of 1997 provided guidance to the NHS on the use and protection of patient, personal, confidential information and emphasised the need for data controllers/ health organisations to have greater controls around the availability and access to patient information. It made a series of recommendations which led to the requirement for all NHS organisations to appoint a Caldicott Guardian who would be responsible for ensuring compliance with the eight Caldicott confidentiality principles. (The principles were revised in December 2020).

6.18 The National Data Guardian (NDG) role was created in 2014 and set in legislation the Health and Social Care National Data Guardian Act 2018. The law placed the NDG role on a statutory footing and granted power to issue official guidance about the processing of health and care data.

In 2017, the Department of Health and Social Care put in policy that all health and social care providers must follow the 10 Data Security Standards. These were developed by the National Data Guardian.

6.19 The national data opt-out was introduced on the 25 May 2018 in line with the NDG's review of Data Security, Consent and Opt-outs. The national data opt-out allows a patient to choose if they do not want their confidential patient information to be used for purposes beyond their individual care and treatment - for research and planning i.e., secondary use purposes. This is aligned with the authorisation used for sharing a patient's data in the Common Law Duty of Confidentiality (CLDC). [NHS Digital operational policy guidance](#) is available.

Caldicott Principles

6.20 The eight principles revised in 2020 are the baseline for good practice;

- Principle 1 – Justify the purpose(s) for using confidential information.
- Principle 2 – Use confidential information only when it is when necessary.
- Principle 3 – Use the minimum confidential information necessary.
- Principle 4 – Access should be on a strict need to know basis.
- Principle 5 – Everyone with access to confidential information should be aware of their responsibilities.
- Principle 6 – Comply with the law.
- Principle 7 – The duty to share information for individual care is as important as the duty to protect patient confidentiality.
- Principle 8 - Inform patients and service users about how their confidential information is used.

Disclosure of Personal Confidential Data

6.21 There are Acts of Parliament that govern the disclosure/ sharing of person-identifiable information. Some make it a legal requirement to disclose whilst others state when information cannot be disclosed. Some examples include:

6.22 Legislation to restrict disclosure

- Abortion Act 1967

- Adoption Act 1976
 - Human Fertilisation and Embryology (Disclosure of Information) Act 1992 and
 - Venereal Diseases Act 1917 and Venereal Diseases Regulations of 1974 and 1992.
- 6.23 Legislation requiring disclosure:
- Births and Deaths Act 1984
 - Education Act 1944 (for immunisations and vaccinations in schools)
 - Police and Criminal Evidence Act 1984 and
 - Public Health (Control of Diseases) Act 1984 & Public Health (Infectious Diseases) Regulations 1985.
- 6.24 Whilst there is a public expectation of appropriate sharing of information between organisations providing health care services to them and with other organisations providing related services, the public rightly expect that their personal data will be properly protected. When sharing personal information, employees must ensure that the Principles of the DPA 2018, the UK General Data Protection Regulation, the Human Rights Act 1998, the Caldicott Principles and the Common Law Duty of Confidentiality are upheld. Information sharing protocols facilitate the exchange of information between organisations.

Keeping individuals informed

- 6.25 It is a legal requirement that individuals are informed how their information is to be used before they are asked to provide it. Where personal information is obtained other than directly from the individual the individual must be provided with privacy information within a reasonable period and no later than one month.

Data Protection Contractual Clauses

- 6.26 The ICB is responsible for obtaining appropriate contractual assurance in respect of compliance with confidentiality, data protection, and transparency requirements from all parties that have access to the ICB's information or conduct any form of information processing on its behalf. This is particularly important where the information is about identifiable individuals. Ensuring this assurance is obtained is a legal requirement under Data Protection legislation. All contractors or support organisations with access to personal data (for which the ICB is data controller) must be identified and appropriate clauses for inclusion in contracts must be in place. These are available under the NHS Standard Contract Particulars – GC21 Conditions or the use of a data

protection protocol as set in the NHS Goods and Non-Clinical Services Contract.

Data Protection Impact Assessments

6.27 Data Protection Impact Assessments (DPIAs) are a tool to support the building of Data Protection Act compliance into projects and initiatives. They are a legal requirement under GDPR.

6.28 DPIAs are part of a "privacy by design" approach and are also intended to prevent privacy related problems from arising, by:

- Considering the impact on privacy at the start of a project
- Identifying ways of minimising any adverse impact
- Building in "privacy by design" from the beginning and throughout the project as it develops.

6.29 The need for Data Protection Impact Assessments should be captured through business case processes and/ or should be considered where any project or proposal will:

- Introduce a new or additional piece of IT that will relate to the management of Personal Confidential Data including pseudonymised information
- Introduce a new process that requires the use of Personal Confidential Data (identifiable data) where it had previously been conducted anonymously
- Involve a change in how the ICB will handle either (a) large amounts of Personal Confidential Data about an individual, or (b) Personal Identifiable Data about many individuals.

6.30 The completion of a DPIA is mandatory under the UK GDPR when processing is "likely to result in a high risk to the rights and freedoms of natural persons".

6.31 Where a high risk is identified that the ICB cannot mitigate, the ICB's DPO is required to notify/consult with the ICO.

6.32 Staff should first use the DPIA screening tool to decide if a full DPIA is needed. If required, they must then complete the ICB issued DPIA template with guidance which is available on the IG Team's intranet site.

Artificial Intelligence

6.33 The ICB supports the responsible and ethical use of Artificial Intelligence (AI) technologies. All AI systems implemented within the ICB must comply with relevant legislation, including Data Protection and Information Governance requirements.

- 6.34 The ICB will follow guidance issued by the Information Commissioner's Office (ICO) and relevant national bodies when implementing AI solutions.
- 6.35 The ICB will not sanction or approve the use of any AI systems or tools that may compromise confidentiality or raise concerns regarding transparency, fairness, or ethical use.
- 6.36 Before any AI system is implemented or used to process personal or special category data, a Data Protection Impact Assessment (DPIA) must be completed and approved.
- 6.37 The ICB acknowledges that AI tools may store user interactions to improve functionality. Information processed by AI systems must remain within approved organisational environments and must not be shared with external providers unless explicitly approved.
- 6.38 Staff must not upload, input or share confidential, personal, or sensitive data with AI tools unless explicitly permitted. This includes personal data, personal confidential data (PCD) and sensitive corporate data.
- 6.39 Employees must ensure they have appropriate rights and permissions to use any data or materials generated by AI tools, including content subject to copyright or other intellectual property restrictions.

7. Equality and Diversity Statement

- 7.1 The Nottingham and Nottinghamshire ICB pays due regard to the requirements of the Public Sector Equality Duty (PSED) of the Equality Act 2010 in policy development and implementation as a commissioner and provider of services, as well as an employer.
- 7.2 The ICB is committed to ensuring that the way we provide services to the public and the experiences of our staff does not discriminate against any individuals or groups on the basis of their age, disability, gender identity (trans, non-binary), marriage or civil partnership status, pregnancy or maternity, race, religion or belief, gender or sexual orientation.
- 7.3 The ICB is committed to ensuring that our activities also consider the disadvantages that some people in our diverse population experience when accessing health services. Such disadvantaged groups include people experiencing economic and social deprivation, carers, refugees and asylum seekers, people who are homeless, workers in stigmatised occupations, people who are geographically isolated, gypsies, Roma and travellers.
- 7.4 As an employer, the ICB is committed to promoting equality of opportunity in recruitment, training and career progression and to valuing and increasing diversity within our workforce.

7.5 To help ensure that these commitments are embedded in our day-to-day working practices, an Equality Impact Assessment has been completed for, and is attached to this policy.

8. Communication, Monitoring and Review

8.1 Following endorsement by the Information Governance Steering Group and ratification by the Audit and Risk Committee, this policy will be communicated to staff via the ICB's Intranet, staff bulletin and published on the [ICB's Website](#).

8.2 Compliance with this policy will be monitored through various requirements of the ICB's Information Governance Management Framework, which is routinely reported to and monitored by the Information Governance Steering Group. Relevant requirements include:

- Data Flow Mapping Registers
- Information Asset Registers
- Information Governance Incident Reports and
- Data Protection Impact Assessment Registers.

8.3 Routine reports on Information Governance are presented to the Audit and Risk Committee. This policy will be reviewed by the Head of Information Governance as required or in light of any legislative changes and at least every three years. The Audit and Risk Committee are responsible for the policy's approval.

9. Staff Training

9.1 Information Governance training is mandatory and all new starters must receive Level 1 Data Security and Protection training as part of their corporate induction.

9.2 All staff members are required to undertake accredited Data Security and Protection training as appropriate to their role. The preferred method is through the e-learning module available through the Electronic Staff Record (ESR) "Data Security Awareness Level 1".

9.3 The ICB has other methods of accessing training:

- e-LfH
- Workbook and Assessment

9.4 Data Security and Protection training must be completed on an annual basis. To achieve competency, employees will have to pass an awareness assessment as part of the training.

- 9.5 The ICB's SIRO, Caldicott Guardian, Information Asset Owners (IAO) and Information Asset Managers (IAMs) also known as Information Asset Administrators (IAAs) may require specific additional training depending on the role they hold. The identified roles requiring additional training and frequency of the training will be set out in the ICB's training needs analysis and plan.
- 9.6 Any individual who has queries regarding the content of this policy or has difficulty understanding how this policy relates to their role, should contact the Information Governance Team by email at nnicb-nn.igteam@nhs.net.
- 9.7 A breach of Data Protection legislation could result in an employee facing disciplinary action. All staff must adhere to ICB policies and procedures relating to the processing of personal information.

10. Interaction with other Policies

- 10.1 This policy should be read in conjunction with relevant sections of the following ICB's policies and supporting procedures.
- Information Governance Management Framework
 - Data Protection by Design Framework
 - Information Security Policy
 - Records Management Policy
 - Freedom of Information and Environmental Information Regulations Policy
 - Internet and Electronic Mail Use Policy
 - Network Security Policy
 - Data Quality Policy.

11. References

- Access to Health Records Act 1990
<http://www.legislation.gov.uk/ukpga/1990/23/contents>
- Confidentiality Advisory Group - Section 251 applications
<http://www.hra.nhs.uk/about-the-hra/our-committees/section-251/>
- Data Protection Act 2018
<http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>
- General Data Protection Regulation (GDPR)
<https://eurlex.europa.eu/eli/reg/2016/679/oj>
- The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019

[The Data Protection, Privacy and Electronic Communications \(Amendments etc\) \(EU Exit\) Regulations 2019 \(legislation.gov.uk\)](#)

- Freedom of Information Act 2000
<http://www.legislation.gov.uk/ukpga/2000/36/contents>
- A Guide to Confidentiality in Health and Social Care 2013
[A Guide to Confidentiality in Health and Social Care - NHS Digital](#)
- Human Rights Act 1998
<http://www.legislation.gov.uk/ukpga/1998/42/contents>
- Information: To share or not to share? The Information Governance Review
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf
- Report on the Review of Patient-Identifiable Information 1997
http://webarchive.nationalarchives.gov.uk/20130124064947/http://www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/@dh/@en/documents/digitalasset/dh_4068404.pdf
- NHS Digital Data Security and Information Governance
[Data security and information governance - NHS Digital](#)

12. Equality Impact Assessment

Name of Policy	Confidentiality and Data Protection Policy
Date of Completion	June 2023, reviewed May 2025
EIA Responsible Person	Head of Information Governance

For the policy, please answer the following questions against each of the Protected Characteristics, Human Rights and health groups:	What are the actual, expected or potential positive impacts of the policy, process, strategy or service change?	What are the actual, expected or potential negative impacts of the policy, process, strategy or service change?	What actions have been taken to address the actual or potential positive and negative impacts of the policy, process, strategy or service change?
Age	There are no actual or expected positive impacts on the characteristic of Age.	There are no actual or expected negative impacts on the characteristic of Age.	None.
Disability¹ (Including: mental, physical, learning, intellectual and neurodivergent)	There are no actual or expected positive impacts on the characteristic of Disability.	There are no actual or expected negative impacts on the characteristic of Disability.	Mechanisms are in place via the Communications and Engagement Team to receive the policy in a range of languages, large print, Braille, audio, electronic and other accessible formats.

Gender² (Including: trans, non-binary and gender reassignment)	There are no actual or expected positive impacts on the characteristic of Gender.	There are no actual or expected negative impacts on the characteristic of Gender.	None.
Marriage and Civil Partnership	There are no actual or expected positive impacts on the characteristic of Marriage and Civil Partnership.	There are no actual or expected negative impacts on the characteristic of Marriage and Civil Partnership.	None.
Pregnancy and Maternity Status	There are no actual or expected positive impacts on the characteristic of Pregnancy and Maternity Status.	There are no actual or expected negative impacts on the characteristic of Pregnancy and Maternity Status.	None.
Race³	There are no actual or expected positive impacts on the characteristic of Race.	There are no actual or expected negative impacts on the characteristic of Race.	None.
Religion and Belief⁴	There are no actual or expected positive impacts on the characteristic of Religion or Belief.	There are no actual or expected negative impacts on the characteristic of Religion or Belief.	None.
Sex⁵	There are no actual or expected positive impacts on the characteristic of Sex.	There are no actual or expected negative impacts on the characteristic of Sex.	None.

Sexual Orientation⁶	There are no actual or expected positive impacts on the characteristic of Sexual Orientation.	There are no actual or expected negative impacts on the characteristic of Sexual Orientation.	None.
Human Rights⁷	There are no actual or expected positive impacts on the characteristic of Human Rights.	There are no actual or expected negative impacts on the characteristic of Human Rights.	None.
Community Cohesion and Social Inclusion⁸	There are no actual or expected positive impacts on the characteristic of Community Cohesion and Social Inclusion.	There are no actual or expected negative impacts on the characteristic of Community Cohesion and Social Inclusion.	None.
Safeguarding⁹ (Including: adults, children, Looked After Children and adults at risk or who lack capacity)	There are no actual or expected positive impacts on the characteristic of Safeguarding.	There are no actual or expected negative impacts on the characteristic of Safeguarding.	None.
Other Groups at Risk¹⁰ of Stigmatisation, Discrimination or Disadvantage	There are no actual or expected positive impacts on the characteristic of Other Groups at Risk.	There are no actual or expected negative impacts on the characteristic of Other Groups at Risk.	None.

Additional Equality Impact Assessment Supporting Information

1. **Disability** refers to anyone who has: "...a physical or mental impairment that has a 'substantial' and 'long-term' negative effect on your ability to do normal daily activities..." (Equality Act 2010 definition). This includes, but is not limited to: mental health conditions, learning disabilities, intellectual disabilities, neurodivergent conditions (such as dyslexia, dyspraxia and dyscalculia), autism, many physical conditions (including HIV, AIDS and cancer), and communication difficulties (including d/Deaf and blind people).

2. **Gender**, in terms of a Protected Characteristic within the Equality Act 2010, refers to: “A person has the protected characteristic of gender reassignment if the person is proposing to undergo, is undergoing or has undergone a process (or part of a process) for the purpose of reassigning the person's sex by changing physiological or other attributes of sex.”
3. **Race**, in terms of a Protected Characteristic within the Equality Act 2010, refers to: A person's colour, nationality, or ethnic or national origins. This also includes people whose first spoken language is not English, and/or those who have a limited understanding of written and spoken English due to English not being their first language.
4. **Religion and Belief**, in terms of a Protected Characteristic within the Equality Act 2010, refers to: Religion means any religion and a reference to religion includes a reference to a lack of religion. Belief means any religious or philosophical belief and a reference to belief includes a reference to a lack of belief.
5. **Sex**, in terms of a Protected Characteristic within the Equality Act 2010, refers to: A reference to a person who has a particular protected characteristic and is a reference to a man or to a woman.
6. **Sexual Orientation**, in terms of a Protected Characteristic within the Equality Act 2010, refers to: Sexual orientation means a person's sexual orientation towards persons of the same sex, persons of the opposite sex or persons of either sex.
7. The **Human Rights Act 1998** sets out the fundamental areas that everyone and every organisation must adhere to. In relation to health and care, the most commonly applicable of the Articles within the Human Rights Act 1998 include: Article 2 Right to Life, Article 5 Right to Liberty and Security, Article 8 Right to Respect of Private and Family Life, and Article 9 Freedom of Thought, Conscience and Religion.
8. **Community Cohesion** is having a shared sense of belonging for all groups in society. It relies on criteria such as: the presence of a shared vision, inclusion of those with diverse backgrounds, equal opportunity, and supportive relationships between individuals. **Social Inclusion** is defined as the process of improving the terms of participation in society, particularly for people who are disadvantaged, through enhancing opportunities, access to resources, voice and respect for rights (United Nations definition). For the EQIA process, we should note any positive or negative impacts on certain groups being excluded or not included within a community or societal area. For example, people who are homeless, those from different socioeconomic groups, people of colour or those from certain age groups.
9. **Safeguarding** means: “...protecting a citizen's health, wellbeing and human rights; enabling them to live free from harm, abuse and neglect. It is an integral part of providing high-quality health care. Safeguarding children, young people and adults is a collective responsibility” (NHS England definition). Those most in need of protection are children, looked after children, and adults at risk (such as those receiving care, those under a DoLS or LPS Order, and those with a mental, intellectual or physical disability). In addition to the ten types of abuse set out in the Health and Care Act 2022, this section of the EQIA should also consider PREVENT, radicalisation and counterterrorism.

10. **Other Groups** refers to anyone else that could be positively or negatively impacted by the policy, process, strategy or service change. This could include, but is not limited to: carers, refugees and asylum seekers, people who are homeless, gypsy, Roma and traveller communities, people living with an addiction (e.g., alcohol, drugs or gambling), people experiencing social or economic deprivation, and people in stigmatised occupations (e.g., sex workers).

Appendix A: Overview of Legislation

The Access to Health Records 1990

This Act gives patient's representatives right of access to their manually held health records, in respect of information recorded on or after 1 November 1991. This Act is only applicable for access to a deceased person's records. All other requests for access to information to living individuals are provided under the access provisions of the Data Protection Act 1998.

Access to Medical Reports Act 1988

This Act allows those who have had a medical report produced for the purposes of employment and/or insurance to obtain a copy of the content of the report prior to it being disclosed to any potential employer and/or prospective insurance company.

Human Rights Act 1998

This Act became law on 2 October 2000. It binds public authorities including Health Authorities, ICBs, and individual doctors treating NHS patients to respect and protect an individual's human rights. This will include an individual's right to privacy (under Article 8) and a service user's right to expect confidentiality of their information at all times.

Article 8 of the Act provides that **'everyone has the right to respect for his private and family life, his home and his correspondence'**. However, this article also states **'there shall be no interference by a public authority with the exercise of this right except as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention or detection of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others'**.

Each organisation must act in a way consistent with these requirements. It must take an individual's rights into account when sharing personal information about them.

Freedom of Information Act 2000

This Act came into force on 1 January 2005. This Act gives individuals right of access to corporate information held by the ICB such as policies, reports, minutes of meetings. The ICB has a Freedom of Information Policy and a nominated officer to deal with requests and queries.

Regulation of Investigatory Powers Act 2000

This Act combines rules relating to access to protected electronic information as well as revising the 'Interception of Communications Act 1985'. The Act aims to modernise the legal regulation of interception of communications in the light of the Human Rights laws and rapidly changing technology.

Crime and Disorder Act 1998

This Act introduces measures to reduce crime and disorder, including the introduction of local crime partnerships around local authority boundaries to formulate and implement strategies for reducing crime and disorder in that local area.

The Act allows disclosure of person identifiable information to the Police, Local Authorities, Probation Service or the Health Service but only if the purposes are defined within the Crime and Disorder Act. The Act does not impose a legal requirement to disclose/exchange person identifiable information and responsibility for disclosure rests with the organisation holding the information.

The Computer Misuse Act 1990

This Act makes it a criminal offence to access any part of a computer system, programs and/or data that a user is not entitled to access. Each organisation will issue individual users an individual user ID and password which will only be known by the individual they relate to and must not be divulged / misused by other staff. This is to protect the employee from the likelihood of their inadvertently contravening this Act.

Each organisation will adhere to the requirements of the Computer Misuse Act 1990 by ensuring staff are made aware of their responsibilities regarding the misuse of computers for personal gain or other fraudulent activities. Any member of staff found to have contravened this Act will be considered to have committed a disciplinary offence and be dealt with accordingly.

The Justice and Coroners Act

This Act has amended the Data Protection Act to strengthen the Information Commissioner's inspection powers.

Appendix B: Overview of NHS Guidance

HSCIC/NHS Digital: Guide to Confidentiality 2013

This code of practice provides detailed guidance for NHS bodies concerning confidentiality and patient's consent to use their personal confidential data. It also details the required practice the NHS must follow concerning security, identifying the main legal responsibilities for an organisation and also details employee's responsibilities.

Employee Code of Practice

Guidance produced by the Information Commissioner detailing the data protection requirements that relate to staff / employee and other individual's information.

The Caldicott Principles

A review of the use of personal confidential data by Dame Fiona Caldicott updated the previous principles. The full report provides guidelines relating to sharing of patient identifiable information and promotes the appointment of a senior health professional to oversee the implementation of the guidance.

Records Management Code of Practice for Health and Social Care 2016

Provides guidance to improve the management of NHS records, explains the requirements to select records for permanent preservation, lists suggested minimum requirements for records retention and applies to all information, regardless of the media, applicable to all personnel within the NHS such as patients, employees, volunteers etc, aids compliance with the Data Protection and Freedom of Information Acts.

ISO/IEC 27001 / 17799 Information Security Standards

These are the accepted industry standards for Information Management and Security and have been adopted by all NHS organisations. It is also a recommended legal requirement under principle 7 of the Data Protection Act.