NHS Derby and Derbyshire Integrated Care Board

NHS Lincolnshire Integrated Care Board

NHS Nottingham and Nottinghamshire Integrated Care Board

Confidentiality and Data Protection Policy

October 2026 – October 2029

Policy purpose
This policy establishes the principles and requirements for protecting confidential information, processing personal data lawfully, and ensuring the appropriate use of information across NHS Derby and Derbyshire Integrated Care Board, NHS Lincolnshire Integrated Care Board and NHS Nottingham and Nottinghamshire Integrated Care Board. It supports compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, amendments introduced by the Data (Use and Access) Act 2025, the Common Law Duty of Confidentiality, the Caldicott Principles, NHS data security requirements, and other relevant information governance legislation, standards and guidance.

CONTROL RECORD	
Title	Confidentiality and Data Protection Policy
Reference number	DLN-IG-003
Version	1.0
Status	Final
Author	DDICB and NNICB Information Governance Teams
Sponsor	Director Corporate Governance and Assurance Director of Outcomes/Senior Information Risk Owner (SIRO)
Team	DLN Information Governance Team
Amendments	N/A
Superseded documents	All predecessor NHS Derby and Derbyshire ICB, NHS Lincolnshire ICB and NHS Nottingham and Nottinghamshire ICB policies, procedures, guidance and associated local documentation relating to confidentiality and data protection.
Audience	All staff working for, or on behalf of, NHS Derby and Derbyshire ICB, NHS Lincolnshire ICB and NHS Nottingham and Nottinghamshire ICB.
Consulted with	Data Protection and Security Steering Group
Equality Impact Assessment	September 2026
Approving body	Audit Committee
Date approved	3 November 2026
Date of issue	November 2026
Review date	October 2029 (or earlier if legislation, national guidance or organisational arrangements change)
Policy retention period	Life of organisations plus six years
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.	

Contents

1. Introduction 4
2. Purpose 4
3. Scope 5
4. Definitions 5
5. Roles and responsibilities 5
6. Policy requirements 6
7. Equality and Diversity Statement 15
8. Communication, monitoring and review 15
9. Confidentiality 16
10. Staff training 17
11. Interaction with other policies 17
12. References 18
13. Equality Impact Assessment 19

Appendix A: Definitions and glossary of terms 23

Appendix B: Overview of legislative framework 25

Appendix C: Identifying personal data 27

1. Introduction

1.1 This policy applies to NHS Derby and Derbyshire Integrated Care Board, NHS Lincolnshire Integrated Care Board and NHS Nottingham and Nottinghamshire Integrated Care Board (collectively referred to as ‘the ICBs’). Each ICB remains responsible for meeting the legal and regulatory obligations that apply to the personal data for which it is a controller.

1.2 The ICBs process information to support the exercise of their statutory functions. This includes personal data (including special category data and criminal offence data), confidential patient and workforce information, and confidential organisational information (including commercially sensitive information). Information may fall within more than one of these categories. Information is a critical organisational asset and must be handled in accordance with legal, regulatory and organisational requirements.

1.3 This policy sets out the ICBs' shared approach to confidentiality, data protection and lawful information use. It supports compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 as amended by the Data (Use and Access) Act 2025, the Common Law Duty of Confidentiality, the Caldicott Principles and relevant NHS and Information Commissioner's Office guidance.

1.4 All individuals working for, or on behalf of, the ICBs have a responsibility to protect information and use it appropriately in accordance with legal, regulatory, professional and contractual requirements.

1.5 Compliance with this policy is mandatory. Failure to comply may result in management, disciplinary or contractual action and, where appropriate, referral to professional, statutory or regulatory bodies.

2. Purpose

2.1 The purpose of this policy is to set out the ICBs' approach to confidentiality, data protection and the lawful, secure and responsible use of information. It explains how the ICBs meet their legal, regulatory and NHS requirements and defines the responsibilities of individuals working for, or on behalf of, the ICBs in protecting and handling information appropriately.

2.2 The policy supports compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025, the Common Law Duty of Confidentiality, the Caldicott Principles and other relevant legal, regulatory and NHS requirements. It also supports the ICBs in embedding confidentiality and data protection requirements into their commissioning, planning, assurance, corporate, workforce and business activities, including information sharing, service

improvement, procurement, digital developments and the management of information risk.

3. Scope

3.1 This policy applies to all individuals working for or on behalf of the ICBs.

3.2 This policy applies to all information processed by or on behalf of the ICBs, regardless of format or location.

3.3 The policy applies throughout the information lifecycle, including the creation, collection, use, storage, sharing, retention, archiving and secure disposal of information.

3.4 The policy applies where the ICBs act as a controller, joint controller or processor of information.

3.5 It should be read in conjunction with related information governance, information security, records management and information rights policies and procedures.

3.6 Any third-party processing information on behalf of the ICBs must comply with applicable contractual, legal and regulatory requirements

4. Definitions

4.1 Definitions of key terms referenced in this policy are described in Appendix A.

5. Roles and responsibilities

5.1 Key responsibilities for specific roles and staff groups are described below:

Role	Responsibilities
ICB Boards and Committees	Provide strategic oversight and seek assurance that confidentiality, data protection and information risk are managed effectively.
Chief Executives	Have overall accountability for ensuring appropriate arrangements are in place for confidentiality, data protection, information governance and information risk management.
Senior Information Risk Owners (SIROs)	Lead and champion information risk management and ensure information risks are identified, assessed, managed and escalated appropriately.

Caldicott Guardians	Provide advice and challenge on the lawful, ethical and appropriate use and sharing of confidential information in accordance with the Caldicott Principles.
Data Protection Officers (DPOs)	Provide independent advice on data protection obligations, monitor compliance, promote good practice and act as a contact point for the Information Commissioner's Office (ICO) and data subjects.
Information Governance Teams	Develop and maintain policies, procedures, guidance, training and assurance arrangements, and provide specialist advice and support.
Information Asset Owners (IAOs)	Maintain oversight of information assets within their area of responsibility, including associated data flows, risks, access controls, retention requirements and assurance arrangements.
Information Asset Administrators (IAAs)	Support Information Asset Owners in maintaining information asset records, data flow documentation and local information governance controls.
Managers	Ensure individuals understand and comply with this policy, complete mandatory training and escalate information governance concerns where appropriate.
Project and Service Leads	Ensure confidentiality, data protection and information governance requirements are considered and embedded within projects, service changes, procurement activities and digital developments.
Procurement and Contract Managers	Ensure appropriate confidentiality, data protection, information security and processor requirements are included within contracts and supplier assurance processes.
All Individuals in Scope	Handle information appropriately, comply with this policy and associated procedures, complete mandatory training, report incidents and raise concerns promptly.

6. Policy requirements

Legal and regulatory compliance

6.1 The ICBs will comply with all applicable legislation, regulatory requirements and national guidance relating to confidentiality, data protection, information governance and information security.

6.2 This includes, but is not limited to, the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 as amended by the Data (Use and Access) Act 2025, the Human Rights Act 1998, the Common Law Duty of

Confidentiality, the Freedom of Information Act 2000, the Environmental Information Regulations 2004, relevant NHS standards and guidance issued by the Information Commissioner's Office (ICO), NHS England and the National Data Guardian.

6.3 Information is a critical organisational asset that supports the effective exercise of the ICBs' statutory functions, good governance, decision-making and accountability. The ICBs will maintain arrangements to demonstrate compliance with legal and regulatory requirements and to support the lawful, secure and responsible management of information.

Data protection principles and accountability

6.4 The ICBs will process personal data in accordance with the principles set out within UK GDPR.

6.5 Personal data must be processed lawfully, fairly and transparently; collected for specified, explicit and legitimate purposes; adequate, relevant and limited to what is necessary; accurate and kept up to date where required; retained only for as long as necessary; and protected through appropriate technical and organisational measures.

6.6 Each ICB is responsible for, and must be able to demonstrate, compliance with these principles. Evidence of compliance may include policies, procedures, training records, privacy information, Data Protection Impact Assessments (DPIAs), information-sharing arrangements, contracts, information asset records, assurance reports and incident records.

Lawful basis for processing

6.7 All processing of personal data must have an identified lawful basis under Article 6 UK GDPR.

6.8 Where special category personal data is processed, an appropriate Article 9 condition and any applicable requirement under the Data Protection Act 2018 must also be satisfied.

6.9 The purpose, lawful basis and any relevant conditions for significant processing activities must be identified and appropriately documented.

6.10 The ICBs recognise that, in carrying out their statutory functions, lawful bases such as public task and legal obligation, and relevant conditions relating to health or social care, public health and substantial public interest, will often be more appropriate than consent.

Common law duty of confidentiality

6.11 The ICBs recognise and will comply with the Common Law Duty of Confidentiality (CLDC).

6.12 All NHS organisations, and those acting on behalf of the NHS, have a duty of confidence to individuals whose information they hold and a responsibility to uphold professional, ethical and legal standards of confidentiality. A duty of confidence arises where information is disclosed or obtained in circumstances where it is reasonable to expect that the information will be kept confidential.

6.13 Confidential information must be used and disclosed only for lawful and legitimate purposes and in a manner that is consistent with the reasonable expectations of the individual concerned.

6.14 Personal data which is also subject to a duty of confidentiality must not be used or disclosed unless there is both an appropriate lawful basis under data protection legislation and an appropriate basis for its use or disclosure under the Common Law Duty of Confidentiality. Such a basis may include:

- explicit consent;
- implied consent, where appropriate and lawful;
- a statutory requirement or statutory power;
- support under the Health Service (Control of Patient Information) Regulations 2002;
- a court order; or
- an overriding public interest justification.

6.15 As commissioning organisations, the ICBs do not provide direct patient care. Consequently, reliance on implied consent for direct care purposes is expected to be limited and careful consideration must always be given to the appropriate legal and confidentiality basis before confidential patient information is used or disclosed.

6.16 Where there is uncertainty regarding the use or disclosure of confidential information, advice should be sought through appropriate Information Governance, Data Protection Officer or Caldicott Guardian arrangements.

Confidentiality and appropriate use of information

6.17 The ICBs are committed to maintaining the confidentiality, integrity and availability of information.

6.18 Individuals working for or on behalf of the ICBs must only access, use, share or disclose information where there is a legitimate business need, an appropriate legal and confidentiality basis and the individual is authorised to do so.

6.19 Access to confidential information must be limited to those with a genuine need to know. The ICBs will ensure that appropriate organisational and technical controls are in place to protect information from unauthorised access, use, disclosure, alteration, loss or destruction.

6.20 Confidential information must be handled in a manner that maintains public trust and confidence in the ICBs' stewardship of information.

Consent

6.21 Consent under data protection legislation and consent under the Common Law Duty of Confidentiality are related but distinct concepts. The appropriate approach depends on the purpose of the processing and the nature of the duty owed.

6.22 Where consent is relied upon as a lawful basis for processing personal data under UK GDPR, it must be freely given, specific, informed and unambiguous. It must be as easy for an individual to withdraw consent as it is to give it.

6.23 Where consent is relied upon to support the use or disclosure of confidential information under the Common Law Duty of Confidentiality, the ICBs will ensure that consent is appropriate to the circumstances and can be evidenced where required.

6.24 The ICBs recognise that consent is not generally the primary lawful basis for undertaking statutory commissioning, governance, corporate or regulatory functions.

6.25 Where processing relies upon consent, appropriate arrangements must exist to record, manage, review and, where applicable, facilitate withdrawal of consent. Consent must be reviewed where the nature, scope or purpose of the processing materially changes.

Caldicott principles and National Data Guardian standards

6.26 The ICBs will apply the eight Caldicott Principles when accessing, using, sharing or disclosing confidential information.

6.27 The Caldicott Principles provide the foundation for the appropriate use and protection of confidential information within health and care organisations. They require organisations to justify the purpose for using confidential information, use it only where necessary, use the minimum information required, restrict access on a need-to-know basis, ensure responsibilities are understood, comply with the law, recognise the importance of appropriate sharing for individual care, and inform patients and service users about how their confidential information is used.

6.28 The ICBs will maintain Caldicott Guardian arrangements and ensure confidential information is managed in accordance with relevant national guidance, including guidance issued by the National Data Guardian.

6.29 Although the ICBs do not provide direct patient care, they recognise the Caldicott principle that the duty to share information appropriately for individual care is as important as the duty to protect confidentiality. This principle will be considered where the ICBs hold or receive information relevant to individual care, safeguarding or another lawful health and care purpose.

6.30 Novel, complex or high-risk decisions involving confidential patient information should be considered through appropriate governance arrangements and, where necessary, escalated to the Caldicott Guardian for advice.

Transparency and privacy information

6.31 The ICBs will provide clear, accessible and transparent privacy information explaining how personal data is collected, used, shared, retained and protected.

6.32 Individuals must be informed how their personal data will be used. Where personal data is obtained from a source other than the individual, privacy information will be provided in accordance with applicable legal requirements and within the timescales prescribed by data protection legislation.

6.33 Privacy information will explain the purposes and lawful bases for processing, relevant information sharing, retention periods, individual rights and routes for queries, concerns and complaints.

6.34 Privacy information will be reviewed whenever there are significant changes to processing activities, technologies, information flows or legal requirements.

Individual rights

6.35 The ICBs are committed to upholding the rights available to individuals under data protection legislation.

6.36 These rights include the right to be informed, access personal data, seek rectification, request erasure where applicable, restrict processing, data portability, object to processing and rights relating to automated decision-making.

6.37 The applicability of individual rights will depend upon the circumstances, lawful basis and purpose of the processing activity.

6.38 The ICBs will maintain arrangements to ensure requests relating to individual rights are recognised and managed fairly, consistently and within applicable statutory timescales.

Data protection by design and DPIAs

6.39 Data protection and confidentiality considerations will be embedded into projects, procurements, service redesigns, digital transformation activities, information-sharing arrangements and new technologies from the earliest stages.

6.40 The ICBs will adopt a data protection by design and by default approach. This means that privacy and confidentiality considerations must be incorporated into the design and operation of systems, services and processes rather than being addressed retrospectively.

6.41 A Data Protection Impact Assessment (DPIA) screening assessment must be completed for new projects, systems, services, information-sharing arrangements, technologies and changes to existing processing activities to determine whether a full DPIA is required.

6.42 Where the DPIA screening assessment identifies that the proposed processing is likely to result in a risk to the rights and freedoms of individuals, a full DPIA must be completed to identify and mitigate those risks before processing begins.

6.43 Where processing is likely to result in a high risk to individuals, a DPIA must be completed before processing begins. Where a high risk cannot be adequately mitigated, the Data Protection Officer must be consulted and consultation with the Information Commissioner's Office (ICO) may be required before processing begins.

Information sharing and disclosure

6.44 The ICBs support the lawful, proportionate and secure sharing of information where it is necessary to fulfil statutory functions, support commissioning activities, population health management, safeguarding responsibilities, public health purposes, service improvement, legal obligations or the wider public interest.

6.45 The requirements that apply will depend on the nature of the information being shared, including whether it constitutes personal data, confidential information, or both.

6.46 Information sharing must be lawful, fair, necessary, proportionate, transparent and secure. When sharing information, the requirements of data protection legislation, the Human Rights Act 1998, the Common Law Duty of Confidentiality and the Caldicott Principles must be upheld.

6.47 The ICBs recognise that there is a legitimate public expectation that information will be shared appropriately to support health and care services and statutory functions. Equally, individuals have a right to expect that their information will be

protected and only shared where there is a lawful, necessary and proportionate reason for doing so.

6.48 Routine or systematic information sharing must be supported by an appropriate documented arrangement. Ad hoc disclosures must be considered on a case-by-case basis and recorded where appropriate. Only the minimum information necessary for the purpose may be shared, using an approved secure route.

Data controllers, joint controllers and processors

6.49 Each ICB remains responsible for personal data for which it acts as a Data Controller.

6.50 Where two or more organisations jointly determine the purposes and means of processing, their respective responsibilities must be defined and documented transparently.

6.51 Where personal data is processed on behalf of an ICB, a written contract or other legally binding arrangement meeting Article 28 UK GDPR requirements must be in place before processing begins. Appropriate assurance must address confidentiality, data protection, security, sub-processing, incidents, individual rights, retention, return or deletion of data and audit.

International transfers

6.52 Personal data must not be transferred outside the UK unless a lawful transfer route applies and the required safeguards and assessments are in place.

6.53 International hosting, remote access and support arrangements must be subject to appropriate Information Governance, procurement and cyber-security consideration.

Artificial intelligence and emerging technologies

6.54 The ICBs support the responsible, lawful and ethical use of artificial intelligence, generative AI, automation, profiling, decision-support and other emerging technologies.

6.55 Such technologies must only be used through approved organisational arrangements and must comply with applicable data protection legislation, confidentiality obligations, information security requirements, equality duties, ethical standards and relevant national guidance.

6.56 The ICBs will not approve or support technologies that compromise confidentiality or present unacceptable risks relating to privacy, transparency, fairness, security or ethical use.

6.57 Personal data and confidential information, including commercially sensitive or otherwise confidential organisational information, must not be entered into unapproved AI systems or public generative AI tools.

6.58 AI-enabled processing must be fair and transparent, include meaningful human oversight where required and be supported by a DPIA where the legal threshold is met. Appropriate rights and permissions must also be in place for data and materials used or generated by AI tools.

Information security and access controls

6.59 The ICBs will maintain appropriate technical and organisational measures to protect information, information assets and information systems against unauthorised or unlawful processing and against accidental loss, destruction or damage.

6.60 Access to information must be role-based, restricted to the minimum necessary for business need, reviewed appropriately and removed when no longer required.

6.61 Individuals must use approved systems, equipment and secure communication methods when handling ICB information and must comply with the ICBs' information security requirements.

6.62 Individuals must not access their own records or the records of family members, colleagues, friends, neighbours or public figures unless access is strictly required for their role and authorised through the appropriate arrangements. Passwords and authentication credentials must not be shared.

Records management, retention and disposal

6.63 Records must be created, maintained, managed, retained, archived and disposed of in accordance with the ICBs' Records Management Policy and the NHS Records Management Code of Practice.

6.64 Information must be retained only for as long as necessary to meet legal, regulatory, operational and business requirements. Records must be securely disposed of when no longer required, unless there is a lawful, regulatory or documented business reason for their continued retention.

Information asset management and data quality

6.65 The ICBs will maintain arrangements for identifying, managing and assuring significant information assets, information risks and data flows.

6.66 Information Asset Owners and Information Asset Administrators must ensure that ownership is clear, records are accurate, risks are identified and information is reviewed when services, systems, suppliers or processing activities change.

6.67 Personal data must be accurate and, where necessary, kept up to date. Information used to support decision-making, statutory functions and business activities must be complete, relevant, reliable and fit for purpose.

Incident management and breach reporting

6.68 The ICBs will maintain arrangements for the prompt identification, reporting, investigation and management of actual or suspected confidentiality, data protection and information security incidents.

6.69 Appropriate action will be taken to contain and mitigate risks, identify lessons learned and meet any reporting obligations to affected individuals, the ICO, NHS England or other relevant bodies.

6.70 The ICBs will promote a culture that encourages prompt reporting, learning and continuous improvement.

National data opt-out

6.71 Where confidential patient information is used for purposes beyond individual care, the National Data Opt-Out will be considered and applied where required by legislation, national policy or relevant guidance.

6.72 Any exemption or non-application must be supported by an appropriate legal basis and documented rationale.

Research, audit, service evaluation and commissioning

6.73 Research, audit, service evaluation, population health management, commissioning and similar activities involving personal data must comply with applicable legal, ethical, professional, NHS and governance requirements.

6.74 Appropriate governance, accountability, transparency and assurance arrangements must be established before processing takes place.

6.75 Before personal data is used for these purposes, the purpose of the activity, controller and processor responsibilities, information required, lawful basis, confidentiality basis, transparency, access arrangements, retention requirements and any necessary approvals must be understood and appropriately documented.

Data protection complaints

6.76 The ICBs will maintain arrangements for receiving, recording, investigating and responding to complaints or concerns about the processing of personal data.

6.77 Complaints will be managed fairly and in accordance with applicable data protection legislation, current ICO guidance and the relevant ICB complaints or information-rights arrangements.

7. Equality and Diversity Statement

7.1 The ICBs pay due regard to the requirements of the Public Sector Equality Duty (PSED) of the Equality Act 2010 in policy development and implementation, as commissioners and providers of services, as well as employers.

7.2 The ICBs are committed to ensuring that the way services are provided to the public and the experiences of staff does not discriminate against any individuals or groups based on 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 ICBs are committed to ensuring that activities also consider the disadvantages that some people in the 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 To help ensure that these commitments are embedded in day-to-day working practices, an Equality Impact Assessment has been completed, and is included within this policy.

8. Communication, monitoring and review

8.1 This policy will be published through each ICB's approved policy publication arrangements and made available to all staff through appropriate communication, training and awareness activities.

8.2 Managers are responsible for ensuring that individuals within their area of responsibility are aware of this policy and understand their obligations in relation to confidentiality, data protection and information governance, including the requirement to recognise and promptly refer information rights requests to the Information Governance Team.

8.3 Compliance with this policy will be monitored through the ICBs' Information Governance assurance arrangements. Monitoring activities may include review of information rights performance, statutory compliance, incidents and personal

data breaches, complaints, risks, mandatory training compliance, Data Protection Impact Assessments (DPIAs), Information Asset assurance, Data Security and Protection Toolkit (DSPT) compliance, audit findings, lessons learned and improvement actions.

8.4 Information relating to compliance with this policy will be reported through the Information Governance Compliance Report to the Data Protection and Security Steering Group and escalated through senior governance arrangements where required.

8.5 Risks relating to confidentiality, data protection and information governance will be managed through the ICBs' Information Governance risk management arrangements in accordance with the Risk Management Policy.

8.6 This policy will be reviewed every three years, or sooner where required by changes to legislation, guidance, organisational arrangements or identified learning.

8.7 Any queries relating to this policy, or how it applies in practice, should be directed to the Information Governance Team.

9. Confidentiality

9.1 All individuals within the scope of this policy have a duty to protect confidential information obtained through the course of their work. This includes information relating to staff, members of the public, individuals whose information is processed by the ICBs, partner organisations, suppliers and the ICBs themselves. Confidential information may include personal data as well as confidential organisational, commercial, contractual, financial or other non-personal information.

9.2 Confidential information must only be accessed, used, shared or disclosed where there is a legitimate business need, an appropriate lawful basis and the individual is authorised to do so as part of their role.

9.3 Individuals must not access their own records, or the records of family members, friends, colleagues, neighbours or public figures, unless this is required for their role and has been authorised through appropriate processes.

9.4 Confidential information must not be discussed in public areas or shared with unauthorised individuals. Information must be handled securely and in accordance with the ICBs' Information Governance policies, procedures and guidance.

9.5 Personal data and confidential information must only be stored, shared and transferred using approved systems, equipment and communication methods. Personal email accounts, unauthorised applications and unapproved devices must not be used for ICB business unless specifically authorised.

9.6 The ICBs will process and protect confidential information in accordance with applicable legislation, including UK GDPR, the Data Protection Act 2018, the Common Law Duty of Confidentiality, the Caldicott Principles and the ICBs' wider Information Governance framework.

9.7 Access to confidential information will be restricted to those with a legitimate business need and controlled through appropriate technical and organisational measures.

9.8 Information must be retained, archived and securely disposed of in accordance with the NHS Records Management Code of Practice and the ICBs' approved retention arrangements.

9.9 Any actual or suspected loss, unauthorised disclosure, inappropriate access, misdirection, alteration, destruction or other breach of confidentiality must be reported immediately through the ICBs' incident reporting arrangements and managed in accordance with the IG incident management process.

10. Staff training

10.1 All individuals working for, or on behalf of, the ICBs must complete mandatory Data Security Awareness training in accordance with organisational requirements.

10.2 Additional confidentiality, data protection and information governance training, guidance or awareness activities may be provided where identified through the ICBs' Information Governance Communication Plan and Training Needs Analysis (TNA).

10.3 The Information Governance Teams will maintain awareness of relevant legislation, regulatory guidance, NHS requirements and emerging good practice and will communicate significant changes where appropriate.

10.4 Compliance with mandatory training requirements and information governance awareness activities will be monitored through the ICBs' Data Protection and Security Steering Group and relevant organisational assurance reporting arrangements.

10.5 Questions regarding this policy or its application should be directed to the relevant Information Governance Team.

11. Interaction with other policies

11.1 This policy should be read in conjunction with the ICBs' wider governance, information governance, records management, information security, risk management and complaint management policies, procedures and guidance.

12. References

12.1 The following legislation, guidance and standards have been taken into account in the development of this policy.

12.2 The Information Governance Teams will apply the most current version of applicable legislation, regulatory requirements, NHS standards and national guidance when implementing and maintaining this policy.

12.3 This reference list is not exhaustive and may be supplemented by additional legislation, case law, regulatory guidance, professional standards or NHS requirements where relevant.

12.4 Key legislation, standards and guidance include:

a) UK General Data Protection Regulation (UK GDPR)

b) Data Protection Act 2018

c) Data (Use and Access) Act 2025

d) Common Law Duty of Confidentiality

e) Health Service (Control of Patient Information) Regulations 2002

f) Freedom of Information Act 2000

g) Environmental Information Regulations 2004

h) Access to Health Records Act 1990

i) Human Rights Act 1998

j) Equality Act 2010

k) Privacy and Electronic Communications (EC Directive) Regulations 2003

l) Computer Misuse Act 1990

m) Health and Social Care Act 2012

n) Health and Care Act 2022

o) National Data Guardian for Health and Social Care Act 2018

p) Information Commissioner's Office (ICO) guidance, codes of practice and regulatory guidance relating to data protection, confidentiality, information sharing, records management, artificial intelligence and information rights

13. Equality Impact Assessment

Date of assessment:	**September 2026**			
For the policy, and its implementation, please answer the questions against each of the protected characteristic and inclusion health groups:	Has the risk of any potential adverse impact on people in this protected characteristic group been identified, such as barriers to access or inequality of opportunity?	If yes, are there any mechanisms already in place to mitigate the adverse impacts identified?	Are there any remaining adverse impacts that need to be addressed? If so, please state any mitigating actions planned.	Are there any positive impacts identified for people within this protected characteristic group? If yes, please briefly describe.
Age[1]	No specific adverse impact identified at draft stage.	The policy applies equally to all individuals and supports consistent protection of personal and confidential information.	None identified at draft stage.	Promotes fair and consistent handling of personal data regardless of age.
Disability (Including: mental, physical, learning, intellectual and neurodivergent)[2]	Potential barriers may arise where policy information, training or communications are not accessible.	Reasonable adjustments, alternative formats and communication support will be provided where appropriate.	Accessibility requirements should continue to be considered when communicating and implementing the policy.	Supports the protection of personal data and confidential information while promoting accessible communication and inclusion.
Gender (including trans, non-binary and gender reassignment)[3]	No specific adverse impact identified at draft stage.	The policy requires personal data to be processed lawfully, fairly and securely and requires confidential information to be protected.	None identified at draft stage.	Supports privacy, dignity and confidentiality for all individuals.

[1] A person belonging to a particular age (for example 32 year olds) or range of ages (for example 18 to 30 year olds).

[2] A person has a disability if she or he has a physical or mental impairment which has a substantial and long-term adverse effect on that person's ability to carry out normal day-to-day activities.

[3] The process of transitioning from one gender to another.

Date of assessment:	**September 2026**			
For the policy, and its implementation, please answer the questions against each of the protected characteristic and inclusion health groups:	Has the risk of any potential adverse impact on people in this protected characteristic group been identified, such as barriers to access or inequality of opportunity?	If yes, are there any mechanisms already in place to mitigate the adverse impacts identified?	Are there any remaining adverse impacts that need to be addressed? If so, please state any mitigating actions planned.	Are there any positive impacts identified for people within this protected characteristic group? If yes, please briefly describe.
Marriage and civil partnership[4]	No specific adverse impact identified at draft stage.	The policy applies consistently regardless of marriage or civil partnership status.	None identified at draft stage.	Supports equitable treatment through consistent confidentiality and data protection practices.
Pregnancy and maternity[5]	No specific adverse impact identified at draft stage.	The policy applies equally to all individuals and requires personal data and confidential information to be handled appropriately and securely.	None identified at draft stage.	Supports the protection of special category personal data and other confidential information, privacy and dignity.
Race[6]	Potential barriers may arise where English is not an individual's first language or communication needs are not recognised.	Alternative formats and communication support will be considered where appropriate.	Communication needs should continue to be considered during implementation.	Supports fair and consistent protection of personal data regardless of race, nationality or ethnic background.

[4] Marriage is a union between a man and a woman or between a same-sex couple.

Same-sex couples can also have their relationships legally recognised as 'civil partnerships'.

[5] Pregnancy is the condition of being pregnant or expecting a baby. Maternity refers to the period after the birth, and is linked to maternity leave in the employment context. In the non-work context, protection against maternity discrimination is for 26 weeks after giving birth, and this includes treating a woman unfavourably because she is breastfeeding.

[6] Refers to the protected characteristic of race. It refers to a group of people defined by their race, colour, and nationality (including citizenship) ethnic or national origins.

Date of assessment:	September 2026			
For the policy, and its implementation, please answer the questions against each of the protected characteristic and inclusion health groups:	Has the risk of any potential adverse impact on people in this protected characteristic group been identified, such as barriers to access or inequality of opportunity?	If yes, are there any mechanisms already in place to mitigate the adverse impacts identified?	Are there any remaining adverse impacts that need to be addressed? If so, please state any mitigating actions planned.	Are there any positive impacts identified for people within this protected characteristic group? If yes, please briefly describe.
Religion or belief[7]	No specific adverse impact identified at draft stage.	The policy applies equally and does not differentiate on the basis of religion or belief.	None identified at draft stage.	Supports equitable and respectful handling of personal data and confidential information.
Sex[8]	No specific adverse impact identified at draft stage.	Personal data must be processed lawfully, fairly, securely and consistently.	None identified at draft stage.	Promotes fair, lawful and secure processing of personal data.
Sexual orientation[9]	No specific adverse impact identified at draft stage.	The policy requires confidential handling of personal data and appropriate safeguards for special category personal data.	None identified at draft stage.	Supports privacy, dignity and confidentiality for all individuals.
Carers[10]	Potential barriers may arise where caring responsibilities	Training materials and guidance can be accessed	Managers should consider individual circumstances when	Supports inclusion and the secure handling of personal

[7] Religion refers to any religion, including a lack of religion. Belief refers to any religious or philosophical belief and includes a lack of belief. Generally, a belief should affect your life choices or the way you live for it to be included in the definition.

[8] A man or a woman.

[9] Whether a person's sexual attraction is towards their own sex, the opposite sex, to both sexes or none. https://www.equalityhumanrights.com/en/equality-act/protected-characteristics

[10] Individuals within the ICB which may have carer responsibilities.

Date of assessment:	**September 2026**			
For the policy, and its implementation, please answer the questions against each of the protected characteristic and inclusion health groups:	Has the risk of any potential adverse impact on people in this protected characteristic group been identified, such as barriers to access or inequality of opportunity?	If yes, are there any mechanisms already in place to mitigate the adverse impacts identified?	Are there any remaining adverse impacts that need to be addressed? If so, please state any mitigating actions planned.	Are there any positive impacts identified for people within this protected characteristic group? If yes, please briefly describe.
	affect access to training or policy awareness activities.	through a range of appropriate routes and formats.	supporting policy awareness and compliance.	data relating to carers and those they support.

Appendix A: Definitions and glossary of terms

Definitions of key terms referenced in this policy are described in the table below:

Term	Definition
Anonymisation	Processing information so that individuals are not identifiable and cannot reasonably be re-identified.
Artificial Intelligence (AI)	Technologies or systems that perform tasks commonly associated with human intelligence, including prediction, classification, generation, recommendation or decision support.
Automated Decision-Making	A decision made solely by automated means without meaningful human involvement.
Common Law Duty of Confidentiality	A legal duty requiring information provided in confidence not to be used or disclosed further without a lawful basis or other valid justification.
Confidential Information	Information, whether personal or non-personal, which is subject to a legal, professional, contractual or other obligation or reasonable expectation of confidentiality. This may include confidential patient and workforce information, commercially sensitive information, contractual or procurement information, financial information and other confidential organisational information.
Commercially Sensitive Information	Information relating to commercial, contractual, procurement or business matters where unauthorised use or disclosure could prejudice the legitimate interests of the ICBs, suppliers, providers or other organisations. Commercially sensitive information may be confidential without constituting personal data.
Confidential Patient Information (CPI)	Information about a patient or service user that identifies them and was provided or obtained in circumstances where confidentiality is expected.
Criminal Offence Data	Personal data relating to criminal convictions and offences, allegations, proceedings or related security measures.
Data Controller	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 Protection Impact Assessment (DPIA)	A process used to identify, assess and minimise data protection risks associated with processing activities.
Data Processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the Data Controller.
Data Subject	The identified or identifiable living individual to whom personal data relates.
Information Asset	A body of information that has value to the organisation and requires ownership, management and protection.
Information Asset Owner (IAO)	The individual responsible for ensuring an information asset is managed, protected and used appropriately throughout its lifecycle.
Information Governance	The framework of legal requirements, standards, policies and procedures that ensure information is handled securely, lawfully, efficiently and effectively.

Term	Definition
Joint Data Controller	Two or more Data Controllers that jointly determine the purposes and means of processing personal data.
National Data Opt-Out	A service that allows patients to opt out of their confidential patient information being used for purposes beyond individual care, where applicable.
Personal Data	Any information relating to an identified or identifiable living individual.
Processing	Any operation performed on personal data, including collection, recording, organisation, structuring, storage, use, disclosure, sharing, transfer, restriction, erasure or destruction.
Pseudonymisation	Processing personal data so that it cannot be attributed to a specific individual without additional information, provided that such information is kept separately and protected by appropriate technical and organisational measures.
Special Category Personal Data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data used for identification, health data, sex life or sexual orientation.
UK GDPR	The United Kingdom General Data Protection Regulation, as incorporated into UK law.

Appendix B: Overview of legislative framework

Access to Health Records Act 1990	Provides specified individuals, including personal representatives and those with a claim arising from a person's death, with rights of access to the health records of deceased individuals.
Access to Medical Reports Act 1988	Provides individuals with rights in relation to medical reports prepared by a medical practitioner for employment or insurance purposes, including the opportunity to view a report before it is supplied.
Caldicott Principles	Provide the ethical and practical framework for the appropriate use and sharing of confidential information across health and care. The principles support justified, necessary, proportionate and lawful information use.
Common Law Duty of Confidentiality	Requires confidential information to be protected and not used or disclosed without an appropriate legal basis, justification or other lawful authority.
Computer Misuse Act 1990	Creates offences relating to unauthorised access to computer systems and data, unauthorised acts intended to impair systems and the unlawful modification of data.
Crime and Disorder Act 1998	Provides a statutory basis for relevant organisations to share information where necessary or expedient for specified crime and disorder purposes. Any disclosure must remain lawful, necessary, proportionate and appropriately documented.
Data Protection Act 2018	Supplements the UK GDPR and provides the wider statutory framework for processing personal data, including special category data, criminal offence data, exemptions, regulatory oversight and enforcement.
Data Security and Protection Toolkit (DSPT)	Provide the NHS assurance framework through which organisations assess and evidence compliance with applicable information governance, data security and cyber security requirements.
Data (Use and Access) Act 2025	Amends the UK GDPR, Data Protection Act 2018 and related privacy legislation, including provisions relating to complaints, automated decision-making and other aspects of data protection compliance.
Environmental Information Regulations 2004	Provide rights of access to environmental information held by public authorities, subject to specified exceptions.
Freedom of Information Act 2000	Provides a statutory right for any person to request recorded information held by public authorities, subject to the application of relevant exemptions.
Health and Care Act 2022	Provides the legislative basis for Integrated Care Boards and their statutory functions, including responsibilities relating to the use and management of information.
Health and Social Care Act 2012	Establishes statutory arrangements relevant to the use and sharing of health and care information and associated NHS functions.

Human Rights Act 1998	Requires public authorities to act consistently with Convention rights, including the right to respect for private and family life, home and correspondence under Article 8.
Information Commissioner's Office (ICO) Codes of Practice	Provide regulatory guidance on complying with data protection and information rights legislation, including accountability, data sharing, data protection impact assessments, individual rights and emerging technologies such as artificial intelligence.
Inquiries Act 2005	Provides the statutory framework for public inquiries and may require the preservation, collection and disclosure of relevant information and records.
National Data Guardian Guidance	Provides statutory and good-practice guidance concerning the use, protection and sharing of health and adult social care information, including the role of the Caldicott Guardian.
National Health Service Act 2006 (including Section 251)	Provides the statutory framework for NHS functions and permits regulations governing the processing of confidential patient information for specified medical purposes where legal requirements are met.
NHS Records Management Code of Practice	Provides the framework for the creation, storage, retention, appraisal and disposal of records and applies to records in all formats.
Privacy and Electronic Communications Regulations 2003 (PECR)	Regulate specified electronic communications activities, including direct marketing, cookies and the security and confidentiality of electronic communications.
Public Interest Disclosure Act 1998	Provides protection for workers making qualifying disclosures concerning specified wrongdoing in the public interest.
Public Records Act 1958	Establishes requirements relating to the preservation, management and disposal of public records.
Regulation of Investigatory Powers Act 2000 and Investigatory Powers Act 2016	Provide the legal framework governing the lawful interception of communications, acquisition of communications data and use of investigatory powers by authorised public authorities.
UK General Data Protection Regulation (UK GDPR)	Establishes the principles, lawful bases, individual rights and accountability requirements governing the processing of personal data.

Appendix C: Identifying personal data

