NHS
Bedfordshire, Luton and Milton Keynes
Integrated Care Board

Data Protection Policy

Document Status:

This is a controlled document. Any printed or downloaded copies are not controlled. The version of this document published on the Bedfordshire, Luton & Milton Keynes Integrated Care Board website is the controlled copy

NHS Bedfordshire, Luton and Milton Keynes (BLMK) Health

Sustainable Development - Environmental

Do you really need to print this document?

Please consider the environment before you print this document and where possible copies should be printed double-sided. Please also consider setting the page range in the print properties, when relevant to do so, to avoid printing the document in its entirety.

Document Control	
Document Owner:	Senior Information Risk Owner
Document Author(s):	Head of Safe Practice & DPO
Directorate:	Medical Directorate
Approved By:	The Board of the Integrated Care Board
Date of Approval:	20-01-2025
Date of Next Review:	20-01-2027
Effective Date:	01-07-2022

Version Control			
Version	**Date**	**Reviewer(s)**	**Revision Description**
v1.0	01-07-2022		The Board of the Integrated Care Board adopted the policy as approved.
Draft V2.0	4-12-2024	Head of Safe Practice & DPO	Minor amendments to the existing contents
V2.0	20-01-2025	Operational Group	The Operational Group approved the minor changes due to the biennial review.

Implementation Plan

Development and Consultation:	The following individuals were consulted and involved in the development of this document: ▪ Information Governance Team (IGT) ▪ Information Governance Group (IGG) ▪ Data Protection Officer (DPO)
Dissemination:	Staff can access this document via the website and will be notified of new / revised versions via the staff briefing. This document will be included in the organisation's Publication Scheme in compliance with the Freedom of Information Act 2000.
Training:	The following training will be provided to make sure compliance with this document is understood: All new staff are required to attend a compulsory Induction Programme which incorporates Information Governance. In addition to this, all staff are required to annually complete and pass the NHS Digital's Data Security Awareness Level 1 module on the Electronic Staff Record (ESR) e-Learning portal. A Training Needs Analysis (TNA) has been developed for staff in key Information Governance roles, as required by the Data Security & Protection Toolkit.
Monitoring:	This policy will be reviewed by its review date or sooner in response to any organisational, regulatory or legislative changes. An assessment of compliance with assertions which make up the Data Security and Protection Toolkit, will be undertaken each year and audited by internal auditors. In addition, the ICBs Information Governance Team will undertake additional monitoring of compliance with this policy as a response to identification of any gaps or as a result of risks identified by incidents, external reviews or other sources of information and advice. This includes regular reporting on the compliance to this policy as part of the Information Governance Framework. Non-conformities to this policy and possible improvements will be discussed in the IGG and appropriate actions will be defined to optimise the information governance.
Review:	The Document Owner will ensure this document is reviewed in accordance with the review date on page 2.

Equality, Diversity and Privacy:	Appendix 1 - Equality Impact Assessment Appendix 2 - Data Protection Impact Assessment
Associated Documents:	The following documents must be read in conjunction with this document as these provide additional guidance on how the data protection policies are implemented within the organisation. Data protection has a direct relation with privacy management and cyber security management and is part of the integrated management system of the organisation. • Information Governance Framework • Information Sharing Policy • Asset Management Policy • Subject Access & Access to Health Records Policy • Records Management & Lifecycle Policy • Social Media Policy • Integrated Risk Management Policy • Offsite Storage Procedures • Controlled Environment for Finance Procedures • Information & Cyber Security Incident Procedure • Working From Home Guidance • Staff IG Handbook
References:	The following articles were accessed and used to inform the development of this document: • Caldicott Principles • A Manual for Caldicott Guardians (2017) • Information: To Share or Not to Share (2013) (Caldicott2) • Review of Data Security, Consent and Opt-Outs (2016) (Caldicott 3)

Table of Contents

1.0 Introduction

1.1 NHS Bedfordshire, Luton and Milton Keynes Integrated Care Board (ICB) aims to ensure robust governance through its formal written procedural documents, such as this document, which communicate standard organisational ways of working. These documents help clarify operational requirements and consistency within day-to-day practice. They can improve the quality of work, increase the successful achievement of objectives and support patient safety, quality and experience. This policy document provides direction and boundaries for using data in the organisation. The ICB aims to ensure its procedural documents are user friendly, up-to-date and easily accessible. For this reason, the documents can contain text that is duplicated from publicly available guidance provided by the NHS or from published laws and regulations.

1.2 The ICB must design and implement procedural documents that meet the diverse needs of our service and workforce, ensuring that none is placed at a disadvantage over others, in accordance with the Equality Act 2010. The Equality Impact Assessment initial screening, which was used to determine the potential impact this policy might have with respect to the individual protected characteristics is incorporated at Appendix 1.

1.3 A Data Protection Impact Assessment is a process which helps assess privacy risks to individuals in the collection, use and disclosure of personal information. The Data Protection Impact Assessment initial screening, which was used to determine the potential impact this policy might have with respect to an individual's privacy is incorporated at Appendix 2.

1.4 The ICB is committed to the delivery of adequate confidential service. This means ensuring that all person identifiable information is processed fairly, lawfully and in a transparent manner.

1.5 The ICB recognises the duty of confidentiality owed to patients, families, staff and business partners with regard to the way in which we process, store, shares and disposes of information.

1.6 In order to operate, the ICB has to collect and use information about people with whom it works, including patients, public, employees (current, past and prospective), clients and customers, and suppliers. This information must be handled and managed appropriately, regardless of how it is collected, recorded and used/processed e.g. on paper or in computer records.

1.7 The obligation to keep personal information secure and to respect confidentiality stems from common law, data protection and human rights legislation and applies to all organisations that process personal identifiable information about living individuals.

1.8 Failure of the ICB to comply with data protection legislation could potentially result in a subsequent investigation by the Information Commissioner's Office, with the

possibility of being fined up to £17.5 million or 4% of our annual turnover, whichever is the greatest for an Information Governance (IG) breach and £8.5 million or 2% of our annual turnover for a breach of the regulation.

1.9 The purpose of this policy is to ensure that all staff understand their obligations with regard to any information they come into contact with, to ensure the ICB meet its legal obligations and NHS requirements concerning confidentiality and information security standards are met.

1.10 This policy is using some specific terms to stipulate the importance of guidelines and directives. These are:

- MUST or SHALL - This indicates a mandatory requirement where compliance is not optional. If not compliant it must be escalated to the highest data protection management level in line with the escalation procedures.
- SHOULD - This indicates a strong recommendation that is to be followed unless there are compelling reasons to deviate. These reasons MUST be justified and verified by the next management level.
- MAY - This indicates that a permission to deviate or an optional action.

2.0 Scope

2.1 This policy applies to all ICB staff members, including Ordinary Members of the Board of the ICB, and Practice Representatives, involved in the ICB's policy-making processes, whether permanent, temporary or contracted-in under a contract for service (either as an individual or through a third-party supplier) - here in after referred to as 'staff'.

2.2 Failure to adhere to this policy may result in disciplinary action and/or referral to the regulatory body to which a staff member may be registered.

2.3 This Policy covers all aspects of information within the ICB, including but not limited to, patient/client/service user information, staff information etc. held in any format e.g. paper, electronic etc.

3.0 Definitions

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

3.2 **Data Controller**

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

3.2.1 The ICB is the Data Controller for the information it holds and is therefore responsible for compliance with data protection law and for ensuring organisations it shares

information with or third parties who process information on its behalf have the appropriate technical and organisational measures in place to protect the information.

3.3 **Joint Data Controllers**

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

3.4 **Data Processors**

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

3.5 **Personal Information**

Personal information is information that identifies an individual or could be used together with other information available to the data controller, to identify an individual.

3.5.1 Examples of personal identifiable data include (but not limited to) name, NHS Number, address, full postcode (even without the remainder of the address), bank details, location data, online identifier (e.g. IP address or cookies), Car Registration Number and digital images (pictures) of a face.

3.6 **Special Category Information**

Special category information is sensitive in nature, therefore needs more protection. However, the ICB's IG and IT Security policies and guidance MUST be applied to personal and special category information.

3.6.1 Examples of Special category information includes (but is not limited to), race, ethnic origin, political views, religion, trade union membership, genetics, biometrics (where used for ID Purposes), health information, sexual activity, sexual orientation and educational data.

3.7 **Pseudonymised and Anonymised Information**

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

3.7.1 Anonymised

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

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

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

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

3.7.4 Pseudonymised

Definition - *"…the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person." - Article 4, GDPR*

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

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

3.7.7 Organisations frequently refer to personal data sets as having been 'anonymised' when, in fact, this is not the case. Staff MUST therefore ensure they consult the ICB IG Team for advice when planning to pseudonymised information.

4.0 Policy Statement

4.1 Data Protection legal obligations and NHS Standards

4.1.1 There are a number of legal obligations and NHS standards placed upon the ICB for the processing of personal identifiable information. These are listed in the ICBs IG Policy & Framework (which must be read in conjunction with this policy), the key ones are listed below.

4.2 The Common Law Duty of Confidentiality

4.2.1 Common Law Duty of Confidentiality is not written in statute. It is based on legal precedent.

4.2.2 The common law duty of confidentiality means that information confided by a patient/service user or otherwise obtained (e.g. during medical examination or when receiving personal care), where it is expected that a duty of confidence applies, should not generally be used or disclosed further, except as originally understood by the confider or with their subsequent permission.

4.2.3 This duty of confidentiality may be set aside, and confidential information disclosed where it is in the public interest or when there is a legal requirement to do so – see Information Sharing Policy

4.3 Human Rights Act

4.3.1 Article 8 of the Human Rights Act establishes the right to respect for an individual's private and family life. Compliance with the Data Protection Act 2018 and the common law duty of confidentiality will satisfy this right.

4.4 UK General Data Protection Regulations & Data Protection Act 2018

4.4.1 The UK General Data Protection Regulations 2021 (UKGDPR) and Data Protection Act 2018 (DPA18) set out the framework for data protection law in the UK.

4.4.2 Data protection laws take a flexible, risk-based approach, which puts the onus on the ICB to think about and justify how and why it uses personal data. It applies to all person identifiable information about living individuals held in any format, including, but not limited to paper documents, computer databases, visual images, audio recordings, CCTV footage, videos, emails etc.

4.4.3 Although UK data protection law applies only to living identifiable individuals, the same level of protection and confidentiality MUST be applied to information about the deceased.

4.4.4 The Information Commissioners Office (ICO) is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. They regulate data protection compliance in the UK promote good practice, monitor breach reports, conduct audits and advisory visits, consider complaints, monitor compliance and take enforcement action where appropriate.

4.5 Caldicott Principles

4.5.1 In 1997 Dame Fiona Caldicott, made a number of recommendations for regulating the use and transfer of patient identifiable information between NHS organisations in England and to non-NHS bodies. This resulted in the Caldicott Principles.

4.5.2 These principles support the legal framework in relation to data protection but have been established specifically with patients in mind and MUST be complied with by ALL NHS organisations in England.

4.5.3 Following a request from the Secretary of State for Health, in 2012 Dame Fiona Caldicott carried out a further review. This resulted in a report, published in 2013, which contained 26 recommendations and this report was known as the Caldicott2 review. One of the recommendations included an added Caldicott Principle:
The duty to share information can be as important as the duty to protect patient confidentiality.

4.5.4 A list of the Caldicott Principles and what they mean can be found in Appendix 3.

5.0 Roles and Responsibilities

The ICBs Information Governance Management Framework (IGMF) documents the roles and responsibilities in relation to Information Governance/data protection and confidentiality. This includes the role of the:

- Senior Information Risk Owner (SIRO)
- Caldicott Guardian (CG)
- Information Asset Owners (IAOs)
- Information Asset Administrators (IAAs)

5.1 Data Protection Officer (DPO)

5.1.1 The DPO supports the ICBs implementation approach to data protection and works closely with and advises the ICB and SIRO in their roles.

5.1.2 They are responsible for providing support and guidance to ICB staff to ensure processing of personal identifiable information is undertaken in line with legal obligations and good practice.

5.1.3 The DPO is responsible for monitoring compliance with data protection law and ensuring data practices comply with applicable legislation and guidance.

5.1.4 The DPO is the primary contact for data subjects (individuals whose data is processed by the ICB) and the Information Commissioners Office (ICO – the body which enforces Information Rights laws and regulations), with whom they are registered.

5.1.5 The DPO reports to the SIRO on relevant matters and to escalate any serious concerns or issues.

5.1.6 The DPO is a legally required role in facilitating ‘accountability’ and the ICB’s ability to demonstrate compliance with data protection law.

5.2 All Staff

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

5.2.2 Staff should note that there is confidentiality clauses in their contract and that they are required to participate in induction, annual mandatory training and comply with the ICBs IG policies and supporting guidance documents.

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

5.2.4 Section 170 (1) of the Data Protection Act 2018: states that it is an offence for a person knowingly or recklessly:
(a) to obtain or disclose personal data without the consent of the controller;
(b) to procure the disclosure of personal data to another person without the consent of the controller, or;
(c) after obtaining personal data, to retain it without the consent of the person who was the controller in relation to the personal data when it was obtained.

5.3 Managers/Heads of Departments

5.3.1 All Managers/Head of Departments within the ICB are responsible for ensuring that their staff are aware of and comply with the ICBs IG policies and supporting standards and guidelines and for ensuring they are built into departmental processes and procedures.

6.0 Processes and Procedures

6.1 Data Protection in Practice

6.1.1 As noted above in section 5 above, the UKGDPR and DPA18 sets out the framework for data protection law in the UK. The sections below therefore provide further information and instructions for staff based primarily on UKGDPR and DPA18.

6.2 Legal Basis for Processing

6.2.1 Personal identifiable information must NOT be processed unless there is a legal basis as listed in UKGDPR under Article 6 – Legal Basis for Processing Personal Information– see Appendix 4.

6.2.2 In addition, where the information is special category information an additional legal basis MUST be identified as listed in UKGDPR under Article 9 – Processing of special categories of personal data – see Appendix 4.

6.2.3 Most (but not all) of the identifiable information processed by the ICB is for the direct care of individuals, therefore the lawful basis for processing will be:

- For personal identifiable information e.g., name, address etc.:
  Article 6(1) (e) – '…exercise of official authority…'
- For the processing of special categories (health) data etc.:
  Article 9(2) (h) – '…health or social care…

6.2.4 When considering new processing or change of purpose for which a legal basis needs to be identified staff MUST consult the ICBs IG Team for advice and support.

6.3 Consent

6.3.1 Consent is one of the six legal bases under UKGDPR, however, direction from the ICO is that health and social care organisations should not use consent for their processing of information if another legal basis exists.

6.3.2 Generally, consent can only be an appropriate lawful basis if a data subject is offered control and is offered a genuine choice regarding accepting or declining the terms offered or declining them without detriment e.g., to take part in medical research etc.

6.3.3 Where consent is the only option it must be informed, explicit and renewed at regular intervals and entitles the data subject to rights which would not be open to them if another legal basis was used e.g., they would have the right to have their information the ICB holds about them to be deleted.

6.4 Data Protection Principles

Article 5 of the UKGDPR sets out 7 basics 'Key Principles' (known as the Data Protection Principles) which lay at the heart of data protection law. Compliance with these principles is therefore a fundamental building block for good data protection practice and key to compliance with data protection law.

- ***Lawfulness, Fairness and Transparency (Principle a)***

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

This means there must:

- be a legal basis for collecting, using and sharing personal and/or sensitive information (see section 6.4 above) and,
- fairness and transparency about what information will be used for.

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

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

In addition to our main Fair Processing Notice, we also add additional notices when required e.g., for the use of information during the Covid 19 pandemic.

- **Purpose Limitation (Principle b)**

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

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

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

For help with assessing the risks associated with processing information staff MUST contact the ICBs IG Team blmkicb.ig@nhs.net.

- **Data Minimisation (Principle c)**

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

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

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

- Clear Data (fully identifiable information).
- Pseudonymised – see section 6.3 above.
- Anonymised – see section 6.3 above.
- Aggregated – where the data is in groups only and cannot be identified down to a Data Subject.

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

- **Accuracy (Principle d)**

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

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

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

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

- **Storage Limitation/Retention (Principle e)**

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

All information should be stored, retained and destroyed in line with the ICBs Records Management & Information Lifecycle Policy & Guidance (based upon the NHS Records Management Code of Practice 2021).

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

- **Integrity and Confidentiality (Principle f)**

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

This principle is also known as the security principle.

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

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

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

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

- **Accountability Principle**

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

The ICB has a number of measures in place including:

- IG & data protection policies as listed in this policy.
- IG & data protection procedures and guidance.
- A privacy by design and default approach – see Data Protection Impact Assessment section below.
- Written contracts in place with organisations that process personal data on the ICBs behalf.
- Maintaining documentation of the ICBs processing activities, including the legal basis for each activity.
- Recording, investigating, learning from and where necessary, reporting personal data breaches.
- Appointment of a DPO as detailed above.
- Requirement for a process in place for all staff to complete the Data Security & Protection staff training on ESR as part of Mandatory Training – see Training section below.
- Fair Processing Notices (the right to be informed) – see Appendix 4.

6.5 Rights of the Data Subject

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

- The Right of Access (Subject Access Request (SAR))
- The Right to Be Informed
- Right to Rectification
- Right to be forgotten
- Right to Restriction
- The Right to Object to Processing
- Automated Decision Making including Profiling
- Portability

6.5.2 The ICB is legally required to process these requests within the 'Time Allowed' of one calendar month. Staff **MUST** therefore refer any enquiries about these rights to the IG Team immediately.

6.6 Information Sharing

6.6.1 As a partner of the Bedfordshire Luton and Milton Keynes Health and Care Partnership, we are signed up to the overarching Information Sharing Agreement (ISA) to support the sharing of patient & service user information for the purpose of direct care under Shared Health and Care Record.

For more information about the Shared Heath and Care Record, please visit **https://blmkhealthandcarepartnership.org/your-health-and-care/shared-health-and-care-record**.

6.6.2 Staff **MUST** make sure they understand the ICBs Information Sharing process and further information on this can be sought from the IG team.

6.7 Data Protection Impact Assessments

6.7.1 A DPIA is a process which helps to identify privacy risks to individuals (data subjects) in the processing of their information.

6.7.2 A DPIA must be carried out for any new or changed processes and systems (for the purpose of this policy, referred to as 'project') where processing of identifiable information is involved.

6.7.3 Failure to identify and implement appropriate privacy protection measures to mitigate risks may result in a breach UKGDPR and DPA18.

6.7.4 There are some projects which do not require a DPIA to be conducted. Completing Stage One of the DPIA process will help you to identify if completion of Stage Two of the DPIA process needs to be completed or not.

6.7.5 All staff MUST make themselves familiar with the DPIA Guidance available in the IG section of the ICB Staff Intranet.

6.8 Reporting Breaches to the ICO

6.8.1 The IG Team must be informed immediately of all IG, privacy, information security and cyber security incidents when these are likely to have a consequence on the confidentiality, integrity, availability of the data, resulting in a risk for the data owner or any individual. These include, but are not limited to, NHSD's classifications:

- Lost in transit
- Lost or stolen hardware
- Lost or stolen paperwork
- Disclosed in error
- Uploaded to website in error
- Non-secure disposal – hardware
- Non-secure disposal – paperwork
- Technical security failing (including hacking)
- Unauthorised access / disclosure

6.8.2 The ICB must report certain personal data breaches to the ICO within 72 hours of becoming aware of the breach (where feasible).

6.8.3 The DPO will report the breach to the ICO without undue delay, unless able to demonstrate, in accordance with the accountability principle, that the breach is unlikely to result in a risk to the rights and freedoms of Data Subjects - see Rights of the Data Subject below.

6.8.4 If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms the ICB must also inform those individuals without undue delay.

6.8.5 For breach reporting procedures please see the ICB Incident & Cyber Security Incident Reporting Procedures available in the IG section of the ICB Staff Intranet.

Appendix 1 - Equality Impact Assessment Initial Screening

Please answer the questions against each of the protected characteristic and inclusion health groups. If there are significant impacts and issues identified a full Equality / Quality Impact Assessment (EQIA) must be undertaken. It is against the law to discriminate against someone because of these protected characteristics. For support and advice on undertaking EQIAs please contact: agcsu.equalities@nhs.net

Name of Policy:	Data Protection Policy
Date of assessment:	14/03/2022
Screening undertaken by:	Head of Information Governance/DPO

Protected characteristic and inclusion health groups. Find out more about the Equality Act 2010, which provides the legal framework to tackle disadvantage and discrimination: https://www.equalityhumanrights.com/en/equality-act/protected-characteristics	Could the policy create a disadvantage for some groups in application or access? (Give brief summary)	If Yes - are there any mechanisms already in place to mitigate the potential adverse impacts identified? If not, please detail additional actions that could help. If this is not possible, please explain why
Age A person belonging to a particular age (for example 32 year olds) or range of ages (for example 18 to 30 year olds).	No	
Disability A person has a disability if she or he has a physical or mental impairment which has a substantial and long-term adverse effect on that person's ability to carry out normal day-to-day activities.	No	
Gender reassignment The process of transitioning from one gender to another.	No	
Marriage and civil partnership Marriage is a union between a man and a woman or between a same-sex couple. Same-sex couples can also have their relationships legally recognised as 'civil partnerships'.	No	
Pregnancy and maternity Pregnancy is the condition of being pregnant or expecting a baby. Maternity refers to the period after the birth and is linked to maternity leave in the employment context. In the non-work context, protection against maternity discrimination is for 26 weeks after giving birth, and this includes treating a woman	No	

unfavourably because she is breastfeeding.		
Race Refers to the protected characteristic of race. It refers to a group of people defined by their race, colour and nationality (including citizenship) ethnic or national origins.	No	
Religion or belief Religion refers to any religion, including a lack of religion. Belief refers to any religious or philosophical belief and includes a lack of belief. Generally, a belief should affect your life choices or the way you live for it to be included in the definition.	No	
Sex A man or a woman.	No	
Sexual orientation Whether a person's sexual attraction is towards their own sex, the opposite sex, to both sexes or none.	No	
Carers Individuals within the ICB which may have carer responsibilities.	No	
Please summarise the improvements which this policy offers compared to the previous version or position.		
Reviewed to take into account UKGDPR and Records Management Code of Practice 2021		
Has potential disadvantage for some groups been identified which require mitigation?		
No – (If there are significant impacts and issues identified a full Equality / Quality Impact Assessment (EQIA) must be undertaken.)		

Appendix 2 - Data Protection Impact Assessment Initial Screening

Data protection is the fair and proper use of information about people. Before completing this form, please refer to the Data Protection Impact Assessment (DPIA) Guidance in the Information Governance (IG) section on the staff Intranet or contact the Data Protection Officer for support via blmkicb.ig@nhs.net

A DPIA is a process to help you identify and minimise the data protection risks. You must do a DPIA for processing that is likely to result in a high risk to individuals. You can use our screening checklist below to help you decide when to do one. If you have answered 'Yes' to any of the 10 screening questions, you must then carry out a full DPIA using the Stage 2 form, which is also available on the Intranet in the IG section.

Name of Policy:	Data Protection Policy
Date of assessment:	14/03/2022
Screening undertaken by:	Head of Information Governance/DPO

Stage 1 – DPIA form **please answer 'Yes' or 'No'**

1.	**Will the policy result in the processing of personal identifiable information / data?** This includes information about living or deceased individuals, including their name, address postcode, email address, telephone number, payroll number etc.	No
2.	**Will the policy result in the processing of sensitive information / data?** This includes for living or deceased individuals, including their physical health, mental health, sexuality, sexual orientation, religious belief, National Insurance No., political interest etc.	No
3.	**Will the policy involve the sharing of identifiers which are unique to an individual or household?** e.g., Hospital Number, NHS Number, National Insurance Number, Payroll Number etc.	No
4.	**Will the policy result in the processing of pseudonymised information by organisations who have the key / ability to reidentify the information?** **Pseudonymised data -** where all identifiers have been removed and replaced with alternative identifiers that do not identify any individual. Re-identification can only be achieved with knowledge of the re-identification key. **Anonymised data -** data where all identifiers have been removed and data left does not identify any patients. Re-identification is remotely possible, but very unlikely.	No
5.	**Will the policy result in organisations or people having access to information they do not currently have access to?**	No
6.	**Will the policy result in an organisation using information it already holds or has access to, but for a different purpose?**	No
7.	**Does the policy result in the use of technology which might be perceived as being privacy intruding?** e.g., biometrics, facial recognition, CCTV, audio recording etc.	No
8.	**Will the policy result in decisions being made or action being taken against individuals in ways which could have a significant impact on them?** Including profiling and automated decision making. (This is automated processing of personal data to evaluate certain things about an individual i.e., diagnosis and then making a decision solely by automated means - without any human involvement)	No
9.	**Will the policy result in the collection of additional information about individuals in addition to what is already collected / held?**	No
10.	**Will the policy require individuals to be contacted in ways which they may not be aware of and may find intrusive?** e.g., personal email, text message etc.	No

Appendix 3 - The Caldicott Principles

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

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

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

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

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

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

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

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

Appendix 4 - Legal Basis for Processing

Article 6 – Legal Basis for Processing Personal Information

a) **Consent:** The Data Subject has given clear consent for the Trust to process their personal data for a specific purpose.
b) **Contract:** the processing is necessary for a contract the Trust have with the Data Subject, or because they have asked us to take specific steps before entering into a contract.
c) **Legal obligation:** the processing is necessary for the Trust to comply with the law (not including contractual obligations).
d) **Vital interests:** the processing is necessary to protect someone's life.
e) **Public task:** the processing is necessary for the Trust to perform a task in the public interest or for its official functions, and the task or function has a clear basis in law.
f) **Legitimate interests:** the processing is necessary for the Trust legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the Data Subject's personal data which overrides those legitimate interests. (This cannot apply if we are a public authority processing data to perform our official tasks.)

Article 9 – Legal Basis for Processing Special Category Information

a) **Explicit Consent** - the data subject has given explicit consent to the processing of those personal data for one or more specified purposes,
b) **Obligations o/ Specific Rights** - processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law.
c) **Vital Interests** - processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
d) **Legitimate Activities** - processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
e) **Already Made Public** - processing relates to personal data which are manifestly made public by the data subject;
f) **Legal Claims** - processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity;
g) **Public Interest** - processing is necessary for reasons of substantial public interest,
h) **Preventative or Occupational Medicine** - processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services.
i) **Public Health** - processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices,
j) **Research** - processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Appendix 5 - Rights of the Data Subject

This appendix includes relevant parts of UKGDPR . Always consult the government websites and the NHS websites on the latest changes of the UKGDPR or contact the IG Team directly.

Right of Access (GDPR Article 15 &Schedule 2, 3 and 4 DPA 2018)

Individuals (data subjects) have the right to:

- Have access to a copy of the information an organisation holds about them, subject to certain safeguards.
- Be provided with a copy of the information held.
- Have the information explained if it is illegible or unintelligible.
- Be informed by any data controller whether personal data of which that individual is the data subject are being processed by or on behalf of that data controller.

Applicants (requesters) do not have to give a reason for requesting access to the information; their motive is irrelevant.

Subject access requests can be made by:

- The data subject (individual) themselves.
- Individuals who have parental responsibility for a child.
- In certain situation a person granted an attorney or agent by the Court of Protection on behalf of an adult who is incapable of consent.
- A representative nominated by the individual to act on their behalf such as solicitors or a relative, where there is valid consent by the individual granting this authority.

For further information about these rights please refer to the ICBs Subject Access & Access to Health Records Policy.

The Right to Be Informed (GDPR Article 13&14)

All individuals have the right to be informed about the collection and use of their personal information. This is a key transparency requirement under the GDPR.

The ICB complies with this right by publishing its fair processing information (also known as Fair Processing Notice) on the ICB public website www.bedfordshirelutonandmiltonkeynes.icb.nhs.uk which individuals should be referred to. However, staff MUST ensure they check the requester has access to the internet, if they don't, they MUST offer to print and post a copy to them.

Right to Rectification (GDPR Article 16)

This is the right for individuals to have inaccurate personal information rectified (corrected) or completed if it is incomplete.

This right is closely linked to the ICB's obligations under the accuracy principle of the GDPR (Article (5)(1)(d)). Personal data is inaccurate if it is incorrect or misleading as to any matter of fact. The ICB is required to take all reasonable steps, including seeking professional opinions where appropriate to establish this.

An individual can make a request for rectification verbally or in writing and the ICB has one calendar month to respond to the request.

In certain circumstances the ICB can refuse a request for rectification.

Right to be forgotten (Erasure) GDPR Article 17 (1)(b)&(e)
The right is not absolute and only applies in certain circumstances. It applies if:

- The personal data is no longer necessary for the purpose which it was originally collected or processed;
- Consent as the legal basis for holding the information and the individual withdraws their consent;
- Legitimate interests is the legal basis for the processing, the individual objects to the processing of their data and there is no overriding legitimate interest to continue the processing;
- The processing is for direct marketing purposes and the individual objects to that processing;
- There is no legal basis to process the information (i.e. in breach of the lawfulness requirement of the 1st principle);
- The ICB has to apply the right to comply with another legal obligation; or
- The ICB has processed the personal information to offer information society services to a child.

Individuals can make a request for erasure verbally or in writing. The ICB has one month to respond to the request.

Right to Restriction (suppression) (GDPR Article 18)
This is not an absolute right and only applies in certain circumstances. This right applies in the following circumstances:

- The individual contests the accuracy of their personal data and the ICB is verifying the accuracy of the data;
- The data has been unlawfully processed (i.e. in breach of the lawfulness requirement of the first principle of the GDPR) and the individual opposes erasure and requests restriction instead;
- The information is no longer need but the individual needs you to keep it to establish, exercise or defend a legal claim; or
- The individual has objected to the ICB processing their data under Article 21(1), and the ICB is considering whether its legitimate grounds override those of the individual.

When processing is restricted, the ICB is permitted to store the personal information, but not use it.

An individual can make a request for restriction verbally or in writing and we have one calendar month to respond to the request.

The Right to Object to Processing (Article 21)
Individuals have an absolute right to stop their information being used for direct marketing. In other cases where the right to object applies, the ICB may be able to continue processing if we can show we have a compelling reason for doing so.

Individuals can object if the processing is for the following, but does not make the right absolute:

- A task carried out in the public interest;
- The exercise of official authority vested in the ICB; or
- The ICB's legitimate interests (or those of a third party).

If the ICB is processing data for scientific or historical research, or statistical purposes, the right to object is more limited.

An individual can make an objection verbally or in writing and we have one calendar month to respond to an objection.

Automated Decision Making including Profiling (Article 22)
The GDPR has provisions on automated individual decision-making (making a decision solely by automated means without any human involvement) and profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.

There are additional rules to protect individuals if the ICB is carrying out solely automated decision-making that has legal or similarly significant effects on them.

The ICB can only carry out this type of decision-making where the decision is necessary for the entry into or performance of a contract, or authorised law applicable to the ICB, or based on the individual's explicit consent.

If the ICB processes personal data in this manner, it must make sure that it gives individuals information about the processing, introduces simple ways for them to request human intervention or challenge a decision and carry out regular checks to make sure that its systems are working as intended.

Portability
The right to data portability gives individuals the right to receive personal data they have provided to the ICB in a structured, commonly used and machine readable format. It also gives them the right to request that the ICB transmits this data directly to another controller.

This right only applies when:

- The lawful basis for processing this information is consent or for the performance of a contract; and
- The ICB is carrying out the processing by automated means (i.e. excluding paper files)