NHS
Bedfordshire, Luton and Milton Keynes
Integrated Care Board

Asset Management 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
www.befordshirelutonandmiltonkeynes.icb.nhs.uk

Sustainable Development - Environmental

Do you really need to print this document?

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

Document Control	
Document Owner:	Chief Finance Officer
Document Author(s):	Head of Safe Practice and Data Protection Officer (DPO)
Directorate:	Medical Directorate
Approved By:	Operational Group
Date of Approval:	03-03-2025
Date of Next Review:	03-03-2027
Effective Date:	03-03-2025

Version Control			
Version	**Date**	**Reviewer(s)**	**Revision Description**
Draft v0.1	29-08-2022	Executive Director	First Draft
Draft v1.0	02-2025	IG Group members	New policy
Final v1.0	03-03-2025	Operational Group	Approved by Operational Group

Implementation Plan

Development and Consultation:	The following individuals were consulted and involved in the development of this document: ▪ Members of the BLMK ICB Information Governance Group ▪ IG & Digital team
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. 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. In addition to this dedicated Information Asset Owner e-learning training is available on the module on the Electronic Staff Record (ESR) e-Learning portal and from the IG team.
Monitoring:	Monitoring and compliance of this document will be carried out via: The BLMK ICB Information Governance Group, with progress reported to the Audit and Risk Assurance Committee. An assessment of compliance with assertions which make up the Data Security and Protection Toolkit (DSPT), will be undertaken each year and audited by internal auditors. In addition, the ICBs Information Governance Department will undertake additional monitoring of compliance with this policy as a response to identification of any gaps or risks identified by incidents, external reviews or other sources of information and advice. The IG team will monitor the review and completion of the Information Asset registers alongside the Information Asset Owners on a biannually basis. This policy will be reviewed annually unless there are changes to legislation resulting in further amendments.
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 BLMK ICB documents must be read in conjunction with this document: ○ Data Protection Policy ○ Information Sharing Policy ○ Information Governance Framework ○ 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: ○ UK General Data Protection Regulation (UKGDPR) ○ Data Protection Act 2018 ○ Data Security Protection Toolkit (DSPT)

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. The ICB aims to ensure its procedural documents are user friendly, up-to-date and easily accessible.

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.

2.0 Scope

2.1 This policy applies to all Integrated Care Board staff members, including Members of the Board of the ICB, involved in policy-making processes, whether permanent, temporary or contracted-in under a contract for service (either as an individual or through a third-party supplier).

3.0 Definitions

What is an Asset?
An asset is anything of value or resource that is owned or controlled by the ICB and is expected to provide future benefits.

An asset can have various forms including:

1. Physical Assets - Material objects with intrinsic value such as buildings, IT-infrastructure and equipment
2. Intangible Assets - Non-physical resources such as intellectual property, brand reputation or image of the ICB or software.
3. Financial Assets - Cash, stocks, bonds, bank accounts and other forms of financial capital that can be used to generate income or investments
4. Information Assets - Valuable data or information, e.g. NHS patient data, intellectual property, proprietary research, or confidential business information. In healthcare, information assets would include patient records, medical research, and any data that supports the organisation's operations.

In the context of Asset Management, people are not considered Assets. People can be seen as valuable resources, critical to the success of the ICB that will handle, generate, or manage the (Information) Assets within Asset Management. People are managed within Human Resource Management processes.

Major information assets are those which are central to the efficient running of the ICB, i.e. patient, finance, stock control etc. Information assets will include computer systems, network, hardware and software as well as manual records that are used to process data.

All major information assets holding information whether manual or electronic, must have an asset register containing relevant file identifications and storage locations.

Assets will have a relation with other Assets. For information assets, it is recognised that these are stored in logical structures such as databases, datastores, data lakes that are representatives of middleware. Information assets are handled, generated and managed using software in the form of applications.

The information assets including any middleware and software, are present within an operating environment of physical systems or computers that will run using operating software and firmware.

These relations are important to the organisation as together they are part of systems that in combination of environmental services, IT services and people, can add value to the ICB. Environmental services include communications, heating, lighting, power, air conditioning and water.

Furthermore, these relations are important to the organisation as all elements of an information system can contain coding that can have vulnerabilities presenting a risk to the ICB.

4.0 Policy Statement

As stated within the BLMK ICB Information Governance Framework, the UK GDPR sets out seven key principles which are all applicable to assets, specifically information assets.

Accountability is one of these key principles in data protection law – it requires organisations to be responsible for complying with the legislation. It requires the ICB to take responsibility for complying with the rest of the principles and to have appropriate processes and records in place to demonstrate that we comply.

One way in which to demonstrate compliance is to implement an asset management policy and process.

To support this implementation and assurance process, the ICB must complete NHS England's Data Security Protection Toolkit (DSPT) which demonstrates compliance with contributing outcomes which require evidence to meet the outcomes.

Several of the outcomes relate to:

1. Information Asset Management
2. Asset Management
3. Third party suppliers
4. Records of processing activities are documented for all uses and flows of personal information.
5. Managing information risks

5.0 Roles and Responsibilities

There are several roles required to ensure structured management arrangements for asset management, in particular, information asset management. Some of the roles are described in more detail in the ICB Information Governance Framework. The following roles and responsibilities are of importance:

The Board of the Integrated Care Board

The Board is accountable for the effectiveness of the Information Governance Framework for BLMK ICB, the compliance to the relevant internal and external laws and regulations as part of the internal control system and for ensuring that the necessary support and resources are available for the effective implementation of the Data Protection Policy and this Information Governance Framework. It has responsibility for the BLMK ICB IG agenda supported by identified senior roles which they are required to appoint including the Caldicott Guardian, Senior Information Risk Owner and Data Protection Officer.

Audit and Risk Assurance Committee (ARAC)

The Audit and Risk Assurance Committee will receive regular IG Reports via the IG Group. The Senior Information Risk Owner is a regular attendee at the Audit and Risk Assurance Committee. The ARAC will also receive the Internal Auditors independent review of the DSPT assessment.

The committee on behalf of the Integrated Care Board, will have oversight on the assurance for the information governance framework.

Information Governance Group (IG Group)

The Information Governance (IG) Group (the Group) is established to support the Chief Financial Officer in their capacity as Senior Information Risk Officer (SIRO). The other activities are described in the ICB Information Governance Framework.

Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner is an executive who is familiar with and takes ownership of the organisation's information risks policy and acts as an advocate for information risk on the Board. This role is described in detail in the ICB Information Governance Framework.

Data Protection Officer (DPO)

When it comes to information asset management and data flow management, the DPO should be consulted on the following:

- whether a DPIA is required;
- how to complete a DPIA;
- whether to outsource the DPIA or resource it in-house;
- what measures and safeguards can be taken to mitigate risks;
- whether the DPOA has been completed correctly; and
- the outcome of the DPIA and whether the processing can go ahead.

The DPO's advice should be recorded on the DPIA. If a decision is taken not to follow their advice, the justification for this should be recorded.

DPOs must also monitor the DPIA's ongoing performance, including how well-planned actions to address risks have been implemented.

Under Article 39 of UK GDPR, DPOs have specific tasks regarding DPIAs. This is why it is important that any responsibilities given to a DPO in relation to a DPIA do not conflict with their ability to complete these tasks in an independent manner, as required by Recital 97.

Information Asset Owners (IAO)
IAOs are generally at director level (senior enough to make decisions concerning their assets), although this role can be delegated to a responsible deputy. They take ownership of their directorate's information assets in the IAR making it their responsibility to ensure that is being maintained.

IAOs should undertake regular reviews to manage the completeness and accuracy of the assets in the asset registers and the information risks associated with these assets. Any medium / high or significant risks / issues should be reported to the SIRO and the IG Group.

This role is described in detail in the ICB Information Governance Framework and appendix 3 details the process (via a checklist) that IAOs must follow.

Information Asset Administrator (IAA)
An IAA can be anyone who uses an information asset as part of their role. They support the IAO by maintaining their delegated part of the Information Asset Register. IAA's must also recognise actual or potential security incidents/threats and consult their IAO on incident management.

The responsibilities of the IAA are described in detail in the ICB Information Governance Framework.

HBLICT
Where ownership of an asset resides with HBLICT, they will be responsible for implementing and maintaining an asset register. No physical assets that have any capability for holding information can be purchased without involvement of the HBLICT Services as all purchases and supply of I.T. hardware equipment must be handled by HBLICT Services. The Information Governance Team should also be advised of any new information assets acquired or changes to existing assets.

Service Asset Owners
Ownership of service-related assets and accountability for them resides with the Director responsible for the area in which the person works. Each owner is responsible for ensuring all new and existing people related assets are correctly reflected in the asset register.

IG Team
The IG team will hold the master organisational information asset register and will prompt IAOs to update it biannually. They will also inform IAOs of any developments relating to completion of training, data protection impact assessment management, data sharing etc.

HR Team
When it comes to leavers, IAOs need to be informed when employees leave the organisation. This will enable IAOs/ IAAs to remove access to the information asset that they manage. IAOs must work with HR to understand who has left to ensure removal. See access management below.

6.0 Processes and Procedures

6.1 Asset management scoping

Assets important to the essential functions of the ICB must be identified and documented. These include:

- Information assets
- Physical / Hardware assets
- Software assets
- Connected medical devices
- Systems storing personal data
- Systems storing business and commercial data

Our IT provider HBLICT, provides an IT service for the ICB, which includes the physical / hardware assets and information assets. They also provide the storage areas for the ICB to save much of the ICBs personal, business and commercial data.

There are several information assets which HBLICT do not manage and these need to be managed by the ICB, for instance these information assets could be online user forms, online content management systems, patient information systems etc.

6.2 Asset registers

All assets must be documented in an asset register as this allows the ICB to identify, classify and manage assets. For information assets the register enables the ICB to monitor the internal flow of data. This facilitates identification of any risks within the different ICB value chains.

Maintenance of the asset register should be done whenever the asset is changed in a way that will have significant influence on the registered classification (Confidentiality, Integrity and availability (CIA) and business criticality) of the asset.

The completeness of the Information asset register must be supported by business impact analysis that will define whether the information asset is part of essential or business critical business processes or data flows.

Assets that are not registered as information assets in the IAR must be registered in general purpose asset register and must be classified for integrity, availability and confidentiality. These assets must be linked to the information assets in the IAR and to the essential processes as defined in the combination with the Record of processing Activities (ROPA) section of the IAR.

Information assets within the asset register must be identified as such as the Information Asset Register (IAR) is a legal requirement. The ICB will use the templates provided by the NHS to identify and define the information assets

The ICB information asset register is be held by the Information Governance Team and the asset register held by HBLICT.

6.3 Critical or essential processes

To define whether a process is critical or essential and should be included in the ROPA, an assessment of the process must take place. The assessment should be in the form of a Business Impact Assessment that will clearly state what the impact is for the ICB when the business process or supporting process is not effective.

The business impact analysis will determine the classification of the process and the assets within the process and will be used to define the requirements for cyber security and business continuity together with risks analysis that will determine the likelihood of ineffective business processes.

Ineffective business processes are processes that for any reason are not functioning according to agreed performance metrics (availability), not producing the correct outcome (Integrity) or are exposed beyond least privilege rules and guidelines (confidentiality).

6.4 Asset risk management

Any asset that is owned or held in custody by the ICB must be assessed for risks. Risk must be identified for the Confidentiality, Integrity and Availability (CIA) of the asset and the consequence or impact of the risks should be based on a Business Impact Assessment (BIA) of the business process in which the asset is present.

The risk assessment should be repeated or updated whenever the assets is changing significantly (that is when the change may result in a different risk classification) or when the environment where the asset is used is significantly changing (that is when the business process in changing or when there are new threats that could have a direct impact on the asset).

The risk assessment process should follow ICB guidelines and best practices and must include the most important stakeholders of the asset and subject matter experts on the process where the assets is present.

The ICB uses the data protection impact assessment templates and guidance to risk assess. The identified risks and mitigation actions should follow ICB standards and guidelines in relation to risk management and should be documented within departmental / corporate risks as per existing ICB risk management processes.

6.5 Access management

Access to any assets should follow the basic access principles as within the HBLICT security and access management policies and must be based on the legal and internal requirements as stated in the ICB Information Governance Framework.

In general, access should be based on least privilege and only for the duration of the activity using the asset. Furthermore, the access must be traceable to a natural person e.g. via system audit.

If access is required to HBLICT managed assets, you must complete the relevant forms via your line manager / HBLICT helpdesk. If access is required to BLMK ICB assets, access will be considered by the Information Asset Owner / administrator.

6.6 Third party or outsources services

When assets owned by the ICB are managed by a third party or service organisation, the accountability of the assets remains with the asset owner.

The asset owner must ensure that the ICB policies and guidelines are followed, and that sufficient assurance is obtained from the third party regarding the adherence to these policies. This should be based on:

- Due diligence of the third party including (cyber) security and privacy management before contracting
- Certification of the third party on relevant management systems (e.g. security management, privacy management, quality management)
- Standard contractual clauses used by purchasing including data processing, security and privacy
- Risk assessment on the actual contract identifying risks related to cyber, information security and privacy aspects on the asset that are not covered by relevant contractual clauses
- Periodic reporting on relevant information security and privacy aspects of the service and the management systems supporting these services
- Internal or third-party assurance reports including the asset specific requirements
- Periodic review and discussion on privacy and security performance and contract risks during the contract lifecycle by a contract management role or delegation

The measures stated should reflect the criticality of the asset and the risk assessment on the contract.

6.7 Audits

To ensure the register remains current, accurate and complete, it will be subject to audit review by the IG Group. IAOs should undertake regular reviews to manage the information risks associated with their relevant assets and record these as appropriate under the guidance of the ICBs risk management process.

In addition, IAOs should audit their information asset users to ensure that any individuals that have left the organisation have been removed.

6.8 Disposal of an Asset

There must be a system in place to ensure all capital asset acquisitions, disposals and transfers are identified, and that the Asset register is amended accordingly.

There should be:

- At least one IAA responsible for updating the relevant Asset register.
- A mechanism in place to ensure that the IAA is informed of all relevant acquisitions, transfers and disposals (i.e., the completion of a standard form)
- A process is in place in respect to recording and monitoring of work in-progress and assets under construction.

HBLICT, have their own Asset Management policy relating to the assets that they manage e.g. laptops, computers, mobile phones etc

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:	Assets Management Policy
Date of assessment:	31/01/25
Screening undertaken by:	Roz Samuel, Head of Safe Practice and 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	No	

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
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.		
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 CCG 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 monitoring of asset registers.		
Has potential disadvantage for some groups been identified which require mitigation?		
No		

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 blmkccg.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:	Assets Management Policy
Date of assessment:	31/01/25
Screening undertaken by:	Roz Samuel, Head of Safe Practice and 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.	Yes
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.	Yes
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.	Yes
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.	Yes
5.	**Will the policy result in organisations or people having access to information they do not currently have access to?**	Yes
6.	**Will the policy result in an organisation using information it already holds or has access to, but for a different purpose?**	Yes
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?**	Yes
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 – Information Asset Owner Checklist

Process
Complete Information Asset Owner training through the ESR or ELfH platforms
Nominate Information Asset Administrators to support you in managing the information asset registers. *(Optional)*
Ensure all Assets and flows are listed on the Information Asset Register and all areas completed. This should be reviewed a minimum of twice a year.
Send your teams Information Asset Register to the Information Governance once you have completed/approved a review.
Ensure a Data Protection Impact Assessment (DPIA) is completed for all Data Processing where necessary. Please see Information governance - ICB Intranet for more details and screening questions.
Review existing DPIA's annually.
Notify the IG team should there be any sharing of information or processing of information by third parties outside of the ICB. This will enable the IG team to consider whether an agreement should be put into place and support you with the development of an Information Sharing Agreements or Data Processing Agreements. This sharing of data or processing of data, could be stated within any contractual agreements e.g. contract, memorandum of understanding, service level agreement etc. The sharing and processing agreements must be signed off with the IG team and you must review existing agreements annually.
Please make sure that all IT systems have been discussed through the Information Governance and Digital Delivery team prior to procurement and that appropriate system support and confidentiality clauses are in place within any relevant contractual documentation including any data processing activities within a data processing agreement.
Please ensure that any risks associated with any data flow (as described within the DPIA) are recorded as per existing risk management policies. For instance, logging these risks on 4Risk and following the risk reporting process.
All user access must be based on the legal and internal requirements as stated in the ICB Information Governance Framework. When it comes to leavers, IAOs must work with HR to understand who has left to ensure removal of access on their IA.
Ensure that when an employee leaves, that the information within the information assets remains and that this is not duplicated or removed by the staff member unintentionally e.g. ensuring all information held on Microsoft Office 365 (SharePoint, NHS mail etc) is transferred to a safe secure area within the ICB infrastructure before they leave and does not remain within their Microsoft Office 365 accounts.