NHS
Bridgewater Community Healthcare
NHS Foundation Trust

Information Asset and System Audit Policy

Policy Number	**IG/Pol/005**
Target Audience	**Information asset owners, information asset administrators, staff looking to procure and enter an agreement with a third party processor, budget holders, staff who access information and business critical assets and systems including finance systems**
Lead Executive Director	**Director of finance/SIRO**
Recommending Committee/Group	**Digital Information Governance and Information Technology (DIGIT)**
Approving Committee(s)	**Corporate Clinical Policy Group**
Ratifying Committee	**Corporate Clinical Policy Group**
Date First Ratified	**February 2012**
Last Full Review Date	**November 2023**
Next Full Review Date	**November 2026**
Extension approved until	**n/a**
Lead Author(s)	**Information Governance Officer/ Information Governance and Records Manager**
Version Number	**5.0**

Applicable Statutory, Legal or National Best Practice Requirements	UK GDPR 2018 and Data Protection Act 2018 Department of Health and Social Care (2021) NHS Digital (2013, updated 2016, 2018) DCB0129 NHS Digital (2013, updated 2016, 2018) DCB0160 NHS Digital (2021) Clinical risk management standards NHS Counter Fraud Authority

The Trust is committed to an environment that promotes equality, embraces diversity, and respects human rights both within our workforce and in service delivery. This document should be implemented with due regard to this commitment.

This document can only be considered valid when viewed via the Trust's intranet. If this document is printed into hard copy or saved to another location, you must check that the version number on your copy matches that of the one online.

Document retention – lifetime of the Trust or 20 year review
Document owner – Information Governance and Records Manager

Version Control Sheet

Version	Date	Reviewed By	Comment
1.0	Feb 12	IG Subgroup	Policy Approval Group
2.0	April 2016 April 2016 April 2016 April 2016	Head of IG Policy Approval Group J. McCartney D. Williams	Minor updates to roles and terminology Approved subject to minor amendments to S. 1, 3, 6, 7.1, 8 & 9 Amendments completed; references updated Final chair approval
3.0	January 2018 April 2018 April 2018 April 2018	IG Subgroup Policy Approval Group J. McCartney S. Arkwright	Minor updates, name changes Approved subject to minor amendments Amendments completed Approved by chair action
4.0	July 2021 December 21 3rd February 2022	Sharon Ramsdale Corporate Clinical Policy Group Trust Board (e-governance)	Full review; supersedes previous policy. Approved, submitted for ratification by the Trust Board Ratified – Policy Officer notified 28/02/2022
4.1	March 2023	S. Ormesher	S. 1 updated to reflect update by NHS England re Digital Technology Assessment Criteria (DTAC) a mandatory requirement for NHS systems
4.2	March 2023	S. Mackie	Amendments approved by chair action
4.3	July 2023	Jackie McKay	Updated to include section 5.9
4.4	July 2023	S. Mackie	Approved by chair action
4.5	August 23	Lucy Brierley	Full review
4.6	Sept 2023	M. Corkery	Reviewed, comments made
4.7	3rd Oct 2023	DIGIT	Approved
4.8	November 2023	Corporate Clinical Policy Group	Approved subject to amendments and final chair approval
4.9	November 2023	Lucy Brierley	Amendments completed
5.0	December 23	J. Cheung	Approved by chair action

Equality impact assessment Consider if this document impacts/potentially impacts: • Staff • Patients • Family members • Carers • Communities	
Yes ☐ **complete box A**	**No** ☒ **complete box B**
Box A Contact the Trust's equality & inclusion manager at: **Email: ruth.besford@nhs.net** **Date contacted:**	**Box B** Complete details below: **Name: Sharon Ormesher** **Email: Sharon.ormesher@nhs.net** **Date: 30.11.21**

Education & professional development (EPD) question

To ensure that any training requirements are discussed, and resources planned and allocated to meet the needs of the service, you must consider whether this document has additional training requirements. Please answer the following question by entering a cross in the Yes or No box below:

	Yes	**No**
Does this document have any additional training requirements or implications?		X

If you have answered **YES** you must forward a copy of this document to EPD **before** submitting to the policy officer.

Date submitted to EPD: ……

No further action is required if you have answered NO.

This table below must be completed in full for audit and governance purposes. Please note documents will be returned if section 1 in the table below is not completed fully. This will result in a delay in listing the document for approval.

Name of document	Information Asset and System Audit Policy
Document number	IG/Pol/005
Document author	Sharon Ormesher

Section 1 - actions required by author	**Authors response**
Date proposal form submitted to policy officer (new documents)	11/10/23
Date proposal form presented to CCPG (new documents)	23/10/23
Date proposal approved by CCPG (new documents)	N/A
Date literature search/reference review requested	N/A
Date EqIA considered	N/A
Date additional training requirements considered	N/A
Date fraud-proofed by the Anti-Fraud Specialist (AFS) if applicable	N/A
Date template accessed on the Hub Add 'OFFICIALSENSITIVE: COMMERCIAL' to front cover if the document can be shared on the internet Add 'OFFICIALSENSITIVE: PERSONAL' to appendices if they include or will include personally identifiable information (PID)	Sept 23
Date literature review completed (check references are formatted correctly, and hyperlinks working)	Sept 2023
Date first draft submitted to policy officer for initial review	31/08/23
Date returned by policy officer following initial review	07/09/23
Date submitted to key individuals/groups/subject matter experts for comments (add names and designations of responders to consultation table)	Sept 2023
For clinical documents, date document submitted to consultation group for sign-off i.e., IPC, Medicines Management (this applies if the document contains medication or medical gases - update version control sheet to confirm sign-off)	N/A
Name of Recommending Committee/group	DIGIT
Date sent to Recommending Committee/group for sign-off	03/10/23
Date signed-off by the Recommending Committee/group (update version control sheet once signed-off)	03/10/23
Date submitted to policy officer for listing at CCPG	05/10/23
Section 2 – for completion by the policy officer	
Date approved by CCPG	13th November 2023
The following policies require Board approval and must be submitted to Board following CCPG approval: • Risk Management Framework Policy • Health & Safety Policy • Policy and procedure for the production, approval and ratification of Trust-wide policies and procedures ("Policy for Policies") Date submitted for Board approval: Date approved by Board:	N/A

Contents

1 Introduction

This document outlines the responsibilities and the process in which Bridgewater Community Healthcare NHS Foundation Trusts (hereafter the Trust) information assets (IA) including Information Systems are maintained and managed. The Trust Information Assets and Information Systems are to be managed in accordance with this policy.

Each information asset within the Trust is to have an information asset owner (IAO) assigned at executive or senior management level; this person is responsible for ensuring the integrity, security, function, and management including any associated agreements, including third party contracts.

NB: It is expected that all IA placed on the information asset register have been through the Trusts due diligence process which includes a digital technology assessment criteria (DTAC), a data protection impact assessment (DPIA), an appropriate agreement and/or contract in place; any health/clinical systems have clinical safety standards, DCB0129 and DCB0160 July 2020.

This will ensure the Trusts data controller responsibilities can be evidenced and monitored within an agreement and/or contract. All IA procured from third parties need to have a written contract with the appropriate Data Processors clauses embedded, to meet legal requirements - see the Information Governance Framework Policy and the Data Protection and Confidentiality Policy for more details.

The role of IAO was created following the UK Government's 2008 review of data handling within Government against the backdrop of high profile data losses. The review focused initially on personal data handling but also covered any sensitive information processed by an organisation.

The recommendations of the review stressed the need to manage IAs in compliance with various statutory obligations it suggested that three new roles be established to facilitate the management of information: senior information risk owner (SIRO), IAO and information asset administrator (IAA).

The IAO role now forms an integral part of the data security and protection toolkit (DSPT) which is an online self-assessment tool that allows organisations to measure their performance against the National Data Guardian's 10 data security standards. All organisations that have access to NHS patient data and systems must use this toolkit to provide assurance that they are practising good data security and that personal information is handled correctly.

1.1 Objective

To ensure all IAs and associated information systems are managed within a legal framework.

To ensure the security and protection and therefore the confidentiality, integrity and availability of the Trust's data. To this end the system/IAA managers should:

- Ensure availability of data when required by users
- Preserve confidentiality

- Ensure that records are protected, complete, accessed and managed in line with information classification and handling arrangements.

- Ensure all audits are undertaken on the information asset are done within a standard format.

1.2 Scope

This policy is applicable to all Trust IAOs, IAAs, budget holders who procure information assets and systems, programmes and project managers.

2 Definitions

The definitions applicable to this policy are as follows:

Active directory	User access to IAs on the Trusts network is controlled mainly by NHS active directory. This is role based. For example, logging into a system using your personal computer (PC) log in or NHS.net address, is the Trusts active directory Therefore if you join or leave the Trust this is managed through the active directory.
Business continuity plan	A business continuity plan is a collection of procedures and information that is developed, compiled, and maintained in readiness for use in the event of a serious incident to enable an organisation to continue to deliver its critical activities at an acceptable pre-defined level.
Decommissioning	Decommissioning is a strategic approach for systematically ending a contract with a data processor who has access to our personal and sensitive information or retiring applications and costly outdated legacy applications without compromising business needs or compliance requirements.
Digital technology assessment criteria (DTAC)	A mandatory requirement that is designed to be used by healthcare organisations to assess suppliers at the point of procurement or as part of a due diligence process, to make sure digital technologies meet our minimum baseline standards. For developers, it sets out what is expected for entry into the NHS and social care.
Disaster recovery plan	A disaster recovery plan is a documented process or set of procedures to protect and recover business IT infrastructure and systems in the event of a disaster. It describes the steps necessary to recover the system to a working state; the acceptable amount of data loss to the business; and how long the recovery is expected to take.

DPIA (data protection impact assessment)	A DPIA is a process to help you identify and minimise the data protection risks of a project. A DPIA must include: • Describe the nature, scope, context, and purposes of the processing. • Assess necessity, proportionality, and compliance measures. • Identify and assess risks to individuals; and • Identify any additional measures to mitigate those risks (Information Commissioner's Office (ICO, 2021).
Information asset	A body of information, defined and managed as a single unit, so that it can be understood, shared, protected, and used effectively. Any collection of personal data required to conduct an organisation's business and the technical equipment to manage this data are referred to as IAs. The term IA is very wide ranging in what it can include any information that is processed, or linked to the IA in an information system will typically contains the following components: • Hardware (linked to IA): computer-based information systems use computer hardware, such as processors, monitors, keyboard, and printers i.e., collecting information (the asset cannot function if the information is not collected) • Software: these are the programs used to organise process and analyse data, e.g., databases, that collect, record and store information • Applications such as Attend Anywhere, Teams. Finance systems that store and hold personal and financial information.
Information asset administrator (IAA)	An IAA may be responsible for the day-to-day management of data. Granting and revoking access to confidential information. Recognising potential or actual security incidents. Consulting the IAO on incident management. If you are a budget holder and access finance systems, you will be identified as an IA administrator for the system.
Information asset owner (IAO)	The responsibility of an IAO is to manage the risks to personal information and business critical information including finance information held within a department and ensuring contracts or agreements are managed.
NHS Counter Fraud Authority (NHSCFA)	The NHSCFA is a special health authority tasked to lead the fight against fraud, bribery and corruption in the NHS.

Processing (of information)	Art.4(2) "Processing" means any operation or set of operations performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Record of processing activities (ROPA)	The record of processing activities allows you to make an inventory of the data processing and to have an overview of what you are doing with the concerned personal data. The recording obligation is stated by Article 30 of the UK General Data Protection Regulation (GDPR).
Robotic Process Automation (RPA)	RPA is a technology that enables the build, deployment, and management of software (robots) that can be programmed to emulate human actions and interact with digital systems in order to automate basic manual and repetitive tasks.
Role based access	A process depending on the user's role they will get access to different parts of the system. Privileged users or systems administrators have higher access to the system therefore by default have access to personal or special category information.
Senior information risk owner (SIRO)	The SIRO will be an executive director or senior management Board member who will take overall ownership of the Trusts Information Risks
System level security	System managers in completing a system level security assessment for each IA. It is the IAA responsibility to complete and regularly review and identify changes to system use and to complete appropriate risk assessments.
Third party access	Third party access to IAs will be based on a formal contract that satisfies all necessary NHS security conditions. Third party suppliers to the Trust and non-Trust devices are not allowed access to the Trust network unless authorised. Where data is shared with third party suppliers, an information sharing agreement must be in place before accounts are created.
Processing (of information)	Art.4(2) "Processing" means any operation or set of operations performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

3 Abbreviations

The abbreviations applicable to this policy are as follows:

CNIO	Chief Nurse Informatics Officer
DIGIT	Digital Information Governance and Information Technology Group
DPIA	Data Protection Impact Assessment
DPG	Digital Programme Group
DPO	Data Protection Officer
DR	Data Recovery
DSCRO	Data Services for Commissioners Regional Office
DSPT	Data Security and Protection Toolkit
ESR	Electronic Staff Record
GDPR	General Data Protection Regulation
HES	Hospital Episode Statistics
IA	Information Asset
IAA	Information Asset Administrator
IAO	Information Asset Owner
ICO	Information Commissioners Office
IG	Information Governance
IT	Information Technology
MFA	Multi-Factor Authentication
MI	Management Information
NHSCFA	NHS Counter Fraud Authority
PC	Personal Computer
PID	Personal Identifiable Data
ROPA	Record of Processing Activities
RPA	Robotic Process Automation
RM	Records Management
SIRO	Senior Information Risk Owner
SUS	Secondary Use Service
TOR	Terms of Reference

4 Other relevant procedural documents

This policy should be read in conjunction with the following documents:

Access Control Policy

Anti-Fraud, Bribery and Corruption Policy

IT Asset Management Policy

IT Acceptable Use Policy (AUP)

Microsoft Office N365 Acceptable Use Policy

Corporate Records (including Document Management) Policy

Data Protection and Confidential Policy

Disciplinary Policy and Procedure

Information Governance Framework Policy

Incident Reporting Policy

Information Security Policy

Mandatory Training and Induction Policy

Performance and Personal Development Review Policy

Procurement Policy

Record Management: Archiving, Retention and Disposal Policy

Records Management: Storing and Movement of Records Policy

Risk Management Framework

Third-Party Supplier Policy

5 Roles and responsibilities

5.1 Senior information risk owner

The SIRO is the Board member who has overall responsibility for information risk management in the Trust including health, staff, finance, and business critical information assets. The responsibilities of the SIRO are to:

- Take overall ownership of the Trust's information risks
- Receive written assurance from IAOs on the required standards within this policy

- Understand how the strategic business goals and how other NHS organisation's business goals may be impacted by information risks, and how those risks may be managed

- Implement and lead the IG risk assessment and management processes regarding procurement

- Sign off and take accountability for risk-based decisions and reviews regarding the processing of personal data within the Trusts registered IAs

- Advise the Board on the effectiveness of information risk management across the Trust.

The SIRO will report to the Quality and Safety Committee on information risks and through the statement of internal controls following assurance from the IAOs.

The SIRO is the director of finance. The deputy SIRO is the assistant director for IT.

5.2 Caldicott guardian

The Caldicott guardian is the chief nurse and is responsible for:

- Ensuring the Trust satisfies the highest practical standards for handling patient identifiable information

- Facilitating and enabling appropriate information sharing and making decisions on behalf of the Trust following advice on options for lawful and ethical processing of information, in relation to disclosures

- Representing and championing information governance (IG) requirements and issues at Board level

- Ensuring confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff

- Overseeing all arrangements, protocols and procedures where confidential patient information may be shared with external bodies both within, and outside, the NHS.

The deputy Caldicott guardian is the deputy chief nurse.

5.3 Assistant director of information technology

The assistant director of IT, supported by the head of IT, the chief nursing informatics officer and the head of information and their teams is responsible for:

- Developing, implementing, and enforcing suitable and relevant information security procedures and protocols to ensure the Trust systems and infrastructure remain compliant with data protection legislation

- Ensuring appropriate usage, accuracy and that reasonable steps are taken to ensure personal data is accurate, having regard to the purposes for which they are processed, are erased, or rectified without delay implement best practices for data quality

- Ensuring all the Trust electronic equipment and assets have adequate security measures to comply with data protection and data security legislation and regulations.

- Any health IT systems on the Trust domain that are used by care professionals is safe and that the organisations have met requirements stated in the two clinical safety standards, DCB0129 and DCB0160 July 2020. These standards are mandatory under the Health and Social Care Act 2012, ultimately, this helps health and care staff to provide better, safer patient care.

5.4 Information asset owner

The IAO is assigned at executive or senior management level; this person is responsible for ensuring the integrity, security, function, and management including any associated contracts and or agreements. Their main responsibilities include:

- Providing assurance to the SIRO on the security and use of these assets on a yearly basis

- Continuing to maintain an understanding of 'owned' assets and how they are used for

- Approving information transfers and giving assurance to the SIRO that these transfers are secure

- Approving and overseeing the decommissioning of the asset (i.e., when the system provider moves from one provider to another)

- Managing the disposal mechanisms for information following the required retention is undertaken to legal standards

- Ensuring any health Information systems not managed by the Trusts IT team are used by care professionals is safe and that the organisations has met requirements stated in the two clinical safety standards, DCB0129 and DCB0160. These standards are mandatory under the Health and Social Care Act 2012, ultimately, this helps health and care staff to provide better, safer patient care

- The appropriate usage, accuracy and that reasonable steps are taken to ensure that personal data is accurate, having regard to the purposes for which they are processed, are erased, or rectified without delay implement best practices for data quality

- Ensuring their IA meets the requirements set out in the DSPT.

- Knowing what information is held and who has access to it for what purpose

- Taking visible steps to ensure compliance with the Trust's IG policies and policies
- Understanding any risks associated with the information asset
- Understanding and addressing the risks to the information asset and provides assurance to the SIRO
- Receiving logs and controls requests from other staff for access to the information asset or assign an appropriate person to act on my behalf
- Ensuring clinical systems meet clinical safety standards
- Ensuring an appropriate person is trained in monitoring clinical system standards and provides relevant support and advice to staff members
- Ensuring changes to the information asset are documented with a formal sign off from the IG department following the undertaking of a DPIA where necessary
- Ensuring risks relating to the IA is managed and mitigated in line with Trust policy
- Leading and fostering a culture that values, protects, and uses information for the benefit of patients
- Appointing an appropriate IAA. NB: if an IAA is not appointed it is expected that the IAA will undertake all responsibilities
- Effective management and security of the Trust's assets including IT resources, for example, infrastructure and equipment
- Developing and implementing a robust IT disaster recovery plan, which is tested annually
- Ensuring IT security levels required by the NHS are met
- Ensuring the maintenance of all firewalls and secure access servers are always in place
- Acting as the IAO with specific accountability services that are operated by corporate and clinical work force, e.g., personal computers, laptops, personal digital assistants and related computing devices, held as an IA
- Working with the IG team and data protection officer (DPO) as appropriate regarding matters relating to data and IT security.
- Support third party access, where required.

5.5 Information asset administrators

IAAs are trained and have working knowledge of the system, their responsibilities include (more details can be found in section 7):

- Ensuring Trust policies including IG, Information Security policies and procedures are followed
- Ensuring any ROPA in relating to the IA and is supplied to the IG team when requested
- Recognising potential or actual security incidents and escalate
- Consulting with the IAO on any incidents and undertake incident management responsibilities
- Ensuring compliance with data sharing agreements
- Ensuring information handling procedures are fit for purpose and properly applied
- Ensuring personal information is not lawfully exploited
- Undertaking a DPIA and manage associated risks and issues where highlighted
- Recognising new information handling requirements and ensuring appropriate procedures are produced and embedded
- Recognising potential or actual security incidents and reporting as per Trust policies
- Reporting to on the current state of the IA
- Ensuring the standards in this guideline are adhered to and monitored.
- Acting as a first port of call for local managers and staff seeking advice on the handling of information
- Ensuring any users of the IA is fully trained and understands the requirements of the system
- Ensuring the IA is only accessed by those who are authorised to do so
- Ensuring access to the IA is always secure and audited and any inappropriate access of the IA is reported via the Trust risk management reporting system (Ulysses).
- Ensuring appropriate procedures/processes are in place to ensure information is managed, accessed and securely destroyed when there is no further requirement for it as per Trust Policy.

5.6 Data protection officer

The DPO for the Trust is held by the Trust secretary. The DPO is responsible for reporting directly to the Board about data protection matters. These may include IG risks to the organisation, privacy concerns or recommendations regarding potential changes to, or new initiatives that, involve processing of personal data.

5.7 Information governance and records manager

With the support of the IG team, the IG and records manager is responsible for:

- Ensuring the information asset register is maintained and updated under the direction of the IAO and the IAA
- Maintaining an awareness of IG issues within the Trust
- Keeping up to date with changes in legislation to ensure the Trust remains compliant
- Reviewing and updating the Information Governance Framework Policy in line with local and national requirements
- Working with IAO, IAA and project managers to complete a DPIA and recommend any areas of risk
- Liaising with wider teams, like IT, procurement, information security and clinical safety to support the IAO, IAA and project managers regarding management of the IA
- Reviewing and auditing all procedures relating to this policy where appropriate
- Ensuring line managers are aware of the requirements of the policy.

The IG and records manager is accountable to the DPO.

5.8 Staff with elevated access/privileged users

Staff with elevated access to IT/Information systems, including clinical systems and health records will be held accountable to the highest standards of use; they will be subject to higher monitoring and will have subsequent enhanced contract agreements – see section 7.3.3.

5.9 Budget holders/team leaders

Budget holders have elevated access to finance IAs and are required to review procedures for financial management to ensure that they meet the standards laid down by the Trust and must comply with the directions and guidance in this document.

Financial performance is a key objective for senior managers within the trust and, as such, failure to comply with budgetary control procedures may be treated as a breach of conduct.

5.10 Digital programme group

The DPG is a sub group of DIGIT. The DPG role is to oversee the governance of digital projects across the organisation and ensure appropriate technical, governance and Information security measure are in place. New projects or changes to existing work programme will be logged with the IT service desk, which will enable auditing and reporting. The group core members are made up of subject matter experts:

- Clinical systems and project team
- Infrastructure/networks team/security
- Service desk team
- Information and data quality team
- IG team
- Finance and procurement teams.

5.11 Digital, Information Governance and Information Technology Group

The DIGIT group will monitor compliance with this policy on behalf of the Trust and will report on the management and accountability arrangement for the policy and provide assurance to the Board through the Trusts sub committees.

6 Equipment

None

7 Corporate register

All IAs are registered by the IG team and must be registered on the Trusts IA register and held centrally by the IG team to maintain corporate oversight and to enable ease of reporting to SIRO and external regulators.

All information assets identified on the register must be classified based on the critical need of the Trust (see appendix two).

Each IAO should develop their business continuity plan based on the IA classification. – see section 7.2.

Note: Some IAs are more critical than others.

7.1 Information asset classification and business continuity plan

Trust IAs are based on three principles of security: 1) confidentiality, 2) integrity, and 3) availability. For each principle, information can be classified as low, moderate, or high.

When classifying the impact, the entity should consider how the information/ information systems is used to accomplish its assigned mission, protect its assets, fulfil its legal responsibilities, maintain its day-to-day functions, and protect individuals. Impact levels are defined as limited, serious, and severe or catastrophic.

The Trust IAs have been classified as platinum, gold and silver and bronze (appendix 2). The classification determines how critical the asset is to the trust business continuity. For all IAs you must have a yearly tested business continuity plan which includes a disaster recovery or a separate document to test the function of the plan and identify any areas for improvement.

7.2 Assessing and classification

IAO/IAA with the appropriate marking to ascertain the types of information the asset holds and how to manage it.

- **Official:** most organisations operate almost exclusively at this level. It is expected that normal security measures will be enforced through local processes and therefore provide sufficient levels of protection to information i.e., staff should be sufficiently aware and understand that they have a responsibility for securely handling any information that is entrusted to them.

- **Official-Sensitive: Personal** - information marked with this classification will be sensitive information relating to an identifiable individual (or group), where inappropriate access could have damaging consequences.

- **Official-Sensitive: Commercial** - information marked with this classification will be commercial or market sensitive information that could have damaging consequences including reputational damage if it were lost, stolen, or inappropriately published.

The classification above has been extracted from the Corporate Records (including Document Management) Policy, there are some examples in this policy, to help with the categorising of the data.

Note: if the IA contains multiple categorised, the highest category is to be used. For example: electronic staff record (ESR) could potentially contain all the above, therefore **Official-Sensitive: Personal** would be applied.

7.3 User process

All IAs must have:

A standard operating procedure to sit under this policy and include:

- A user process that assigns different levels of access, i.e., role-based access, to ensure information is only accessed by those who need to access it
- A process that adds and removes authorised users, this includes levels of authorised access to ensure access rights are removed immediately and to give access to those in a timely manner
- A guide on how to use the IA safely ensuring the information remains secure.

7.3.1 Monitoring

All IA must have a process that monitors users access to ensure no authorised access by users. This can be undertaken by the IAA, or a team assigned. If inappropriate access is discovered, the incident managed process is to be followed.

For business-critical information assets such as a finance system, regular monitoring of activity should be undertaken.

7.3.2 Training

All IA must have a training schedule based on the level of access of the user to ensure users know their responsibilities and are able to do their job efficiently.

7.3.3 Privileged access

Staff with elevated/privileged access to an IA have a greater responsibility and are held accountable to the highest standards of use. Their responsibility for having elevated/privileged access must be addressed at each performance and personal development review (PPDR), or those set by the IAO.

A suggested template to support this can be found in appendix 1 – also see 5.3 in responsibilities.

7.4 Data flows/record of processing (ROPA)

Information that is transferred in and out of the IA must be recorded, retained, and audited yearly to ensure information has been legally shared. All transfers forms (bulk data transfers) are held with the IG team.

7.5 Third party transfers

It is a legal requirement that an agreement and/or contract must be in place prior to sharing information with a third party/outside the Trust.

Any third-party transfers (information in and out) must be authorised by the IAO or equivalent (Caldicott guardian or SIRO), as per the Data Protection and Confidentiality Policy.

You should consult the Anti-Fraud, Bribery and Corruption Policy if entering a contract with a third party where there is a potential for fraud or suspected fraud.

7.6 Quality of information

The quality of the information contained in the asset must be audited and reviewed on a scheduled programme of improvement, as per the Data Protection and Confidentiality Policy.

Where third party access is required, this must be registered and scheduled in line with IT services can schedule and support the third-party access.

For business-critical information assets such as a finance system, regular monitoring of activity should be undertaken.

7.7 Password complexity meeting cyber security standards

Where an IA is accessed through the user access directory set by the Trusts IT Team, this must comply with cyber security standards. Where an IA/system is not managed in this way, it must have a password procedure based on the information contained in the Access Control Policy; this is a DPST requirement.

The IA must use access security settings approved by the Trusts Information Security Team to ensure there are no security issues identified.

Any IA that sends or receives information via electronic transfer must ensure it is encrypted/secure. All paper flows of information containing personal identification data (PID) must be tracked and secure as per record management (RM) standards.

7.8 Robotic process automation

Information that is processed via RPA must be structured and digitised data. When implementing RPA, it has to be supported by local procedures or business continuity plans as part of the IA. IT is recommended that a DPIA is completed for each RPA process. Each RPA process is approved by RPA Board and QIA is completed to ensure patient /clinical safety.

RPA imitates activities carried out by humans. Allowing automation of high volume, rule-based, repeatable tasks.

7.9 Multi-factorial authentication

MFA is widely recognised as one of the most effective ways to protect data and accounts from unauthorised access. The NHS England Policy sets out the standards regarding enabling MFA digital systems throughout the health sector, with particular requirements on assets that are remotely accessible or have privileged access to systems.

7.10 Risks

Any risks associated with the IA must be registered on the Trust corporate risk register.

All incidents reported on the IA must be reported on the Trusts risk management reporting system (Ulysses) and managed as per the Incident Reporting Policy.

7.11 Fraud, bribery and corruption in the NHS

Fraud is an act of deception that is intended to make a financial gain or to cause loss to another party. Bribery is generally defined as the giving or receiving of a financial or other advantage in exchange for improperly performing a relevant function or activity.

The maximum penalty for fraud and bribery is 10 years imprisonment, with an unlimited fine. All suspicions of fraud, bribery and corruption should be reported to the Trust's nominated Anti-Fraud Specialist.

7.12 Retention and disposal

To comply with legal requirements, the IA must have a retention and disposal process in line with the Trust Records Management: Archiving, Retention and Disposal Policy.

8 Consultation

Key individuals/groups involved in the development of the policy to ensure it is fit for purpose once approved:

Name	Designation
Sharon Ormesher	Information Governance and Records Management Manager
Jackie McKay	Senior Information Governance Officer
Lucy Brierley	Information Governance Officer
Mary Corkery	Policy Officer
Information Asset Owners	Distributed to registered IAO
Information Asset Administrators	Distributed to registered IAA
Razia Nazir	Knowledge and Library Services Manager
Phillip Leong	Anti-Fraud Specialist Mersey Internal Audit Agency
Katherine Summers	Infection Prevention and Control Lead Nurse
Rachel Hall	Head of Research
Rachel Hurst	Deputy Director of Finance
Denise Winstanley	Senior Administrator
Kati Wright	Digital Project Manager
Sandra Alderson	Programme Manager
Alan Tweddell	Head of IT
DIGIT	
Corporate Clinical Policy Group	

9 Dissemination and implementation

9.1 Dissemination

This policy will be disseminated by the IG records manager to all registered IAO and IAA members of the DIGIT and Digital Programme Group.

The policy will be made available on the Trust intranet and internet and published in the team brief.

9.2 Implementation

This policy will be implemented through the DSPT and the audit programme.

10 Process for monitoring compliance and effectiveness

Process for reviewing compliance and effectiveness i.e., audit, review, survey, incident reporting	Responsible	Frequency of monitoring	Assurance group
DSPT assessment of information submitted	Annually for sign-off	Annual	DIGIT
Incident analysis	Monthly/ quarterly	IG report to DIGIT	DIGIT

11 Standards/key performance indicators

Audit programme based on the standards set in this policy.

Note: The audit tools associated with this policy will be held with the IG team, as the tools will be piloted and enhanced based on action plans.

12 References

Data Protection Act 2018 c. 12 [online]. Available at: http://www.legislation.gov.uk/ukpga/1998/29/contents

Department of Health and Social Care (2016) Records Management: code of practice for health and social care [online]. Available at: https://www.gov.uk/government/publications/records-management-code-of-practice- for-health-and-social-care

Health and Social Care Act 2012 c. 7 [online]. Available at: https://www.legislation.gov.uk/ukpga/2012/7/contents/enacted

Information Commissioner's Office (ICO) (nd) Data protection impact assessments [online]. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/
Accessed on 30/11/21

Information Commissioner's Office (ICO) What do we need to document under Article 30 of the UK GDPR? [website]. Available at: https://ico.org.uk/for- organisations/guide-to-data-protection/guide-to-the-general-data-protection- regulation-gdpr/documentation/what-do-we-need-to-document-under-article-30-of- the-gdpr/

NHS Digital (2013, updated 2016, 2018) DCB0129: Clinical Risk Management: its Application in the Manufacture of Health IT Systems [online]. Available at: https://digital.nhs.uk/data-and-information/information-standards/information- standards-and-data-collections-including-extractions/publications-and- notifications/standards-and-collections/dcb0129-clinical-risk-management-its- application-in-the-manufacture-of-health-it-systems

NHS Digital (2013, updated 2016, 2018) DCB0160: Clinical Risk Management: its Application in the Deployment and Use of Health IT Systems [online]. Available at: https://digital.nhs.uk/data-and-information/information-standards/information- standards-and-data-collections-including-extractions/publications-and- notifications/standards-and-collections/dcb0160-clinical-risk-management-its- application-in-the-deployment-and-use-of-health-it-systems

NHS Digital (2021) Clinical risk management standards [online] Available at: https://digital.nhs.uk/services/clinical-safety/clinical-risk-management-standards Accessed 28/10/21]

NHS Digital (2020) DCB0129: Clinical Risk Management: its Application in the Manufacture of Health IT Systems [online]. Available at: https://digital.nhs.uk/data-and-information/information-standards/information-standards-and-data-collections-including-extractions/publications-and-notifications/standards-and-collections/dcb0129-clinical-risk-management-its-application-in-the-manufacture-of-health-it-systems

NHS Digital (2020) DCB0160: Clinical Risk Management: its Application in the Deployment and Use of Health IT Systems [online]. Available at: https://digital.nhs.uk/data-and-information/information-standards/information-standards-and-data-collections-including-extractions/publications-and-notifications/standards-and-collections/dcb0160-clinical-risk-management-its-application-in-the-deployment-and-use-of-health-it-systems

Cabinet office, Sir G O'Donnell (2008) Data Handling Procedures in Government: Final Report [online]. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60966/final-report.pdf.
Accessed 26/09/23.

NHS Digital (2022) Data Security Standard 10 - Accountable suppliers [online]. Available at: https://digital.nhs.uk/cyber-and-data-security/guidance-and-assurance/data-security-and-protection-toolkit-assessment-guides/guide-10---accountable-suppliers

NHS England (2023) Multi-factor authentication (MFA) policy [online] Available at: https://digital.nhs.uk/cyber-and-data-security/guidance-and-assurance/multi-factor-authentication-mfa-policy

Privilege users example

Consider using this form as evidence of ensuring those with elevated access, know their obligations. It is recommended it is used when undertaking their annual PPDR.

Name	
Date of PPDR	

As a System administrator and/or a user with privileged access you have elevated rights compared to a normal user. This includes access to sensitive information which you would not normally be required to see as part of your role.

All systems within the trust, containing sensitive information are periodically reviewed and monitored to confirm no unauthorised access is being made.

To protect the integrity of all data in ensuring that information is only ever accessed, as the need arises, in your role as system administrator you are asked to confirm the following statements:

- All actions undertaken whilst working with sensitive data are taken with highest level of integrity in terms of respect of the confidentiality, integrity or availability of the systems I support.
- As system administrator I understand the responsibility in that all work should be undertaken in the knowledge of the appropriate system access policies and compliance with IG standards.
- I understand that as a system administrator if I use data illegally/for my own gain, I could face disciplinary action which may lead to prosecution.

Manager's name	
System users' signature (digital signature can be used)	

Information asset classification

IA classification (based on service provision)	Service characteristics/provision
Platinum	• Typically, critical national services. • Absence of system leads to complete failure of dependent systems and services with a high possibility of clinical safety issues. • Service interruption results in severe reputational damage. • 24x7x365 support required. • Service availability – 99.9%. • Data Recovery (DR) recovery target 2 hours. • Monthly management information (MI) reporting. • Example service – Spine.
Gold	• Predominantly transactional services. • Absence of system leads to operational difficulties that can be coped with for a limited period. • Absence of system may lead to increased risk to clinical care. • 8am-6pm Monday to Saturday support required. • Service availability – 99.9%. • DR recovery target 4 hours. • Monthly MI reporting.
Silver	• Predominantly data capture, batch processing. • Absence of system leads to operational difficulties, but these are manageable for an extended period e.g., 1day. • Absence of system may lead to a slight increase in clinical risk business hours support (8am-6pm) Monday to Friday (not Bank holidays). • Service availability – 99.5%. • DR recovery optional - dependent on outcome of business impact analysis. • Monthly MI reporting. • Existing service – Secondary Use Service (SUS), Hospital Episode Statistics (HES).
Bronze	• Business hours support (8am-6pm) Monday to Friday (not Bank holidays). • Service availability – 98%. • DR recovery optional - dependent on outcome of business impact analysis. • Ad Hoc MI reporting. • Existing service – Parliamentary questions/publications.