University Hospitals of Derby and Burton
NHS Foundation Trust

TRUST POLICY FOR INFORMATION GOVERNANCE

Reference Number IG 2010 002	**Version: 3.2**		**Status** Final	**Author:** Nic Laban **Job Title:** Head of Information Governance/Data Protection Officer
Version / Amendment History	**Version**	**Date**	**Author**	**Reason**
	1.1	Sept 2009	D Leafe	Amendment
	2.4	Jan 2022	A Woodhouse	Policy review and minor amendments
	3.0	Jun 2022	E Griffiths	Policy review, updates, refined title. Removed appendices.
	3.1	Sep 2023	E Griffiths	Updated group and organisation names, adding two deputy roles
	3.2	Oct 2024	N Laban	Policy review and minor amendments

Intended Recipients: All staff, volunteers and third-party contractors.

Training and Dissemination: Training will be delivered to all new staff on Trust induction and to existing staff on mandatory training days. Face to Face, E-learning and Podcast is available. The Policy will be published on Trust intranet (Net-i).

To be read in conjunction with: Trust Disciplinary Procedures, Policy for Data Protection & Dealing with Confidential Information, Freedom of Information Policy, Patient Access Policy, Data Quality Policy, Information Technology and Cyber Security Policy, Records Management Policy.

In consultation with and Date: Information Governance, Cyber Security and Disaster Recovery (IGCSDR) November 2024.

EIRA Stage One Completed **Yes**

Stage Two Completed **Yes**

Stages 1-4 Completed 15/8/22

The equity and health inequality implications for people from protected characteristics or who are under-represented have been considered in line with the Trust's People EIRA. The information supporting this policy evidences that there are no issues or barriers which could impact people from the protected characteristic groups, however some SOPs under the policy may need amending to ensure data from or for protected groups is used fairly.

Approving Body and Date Approved	Trust Delivery Group 23 December 2024
Date of Issue	November 2024
Review Date and Frequency	November 2025

Contact for Review	Head of Information Governance/DPO
Executive Lead Signature	Executive Chief Digital Information Officer

Contents

TRUST POLICY & PROCEDURE FOR INFORMATION GOVERNANCE

1 Introduction

Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources. It plays a key part in clinical governance, service planning and performance management.

Information Governance is a framework that brings together all the statutory and mandatory requirements and best practice that apply to the handling of information to ensure compliance with the law. Information Governance is also a component of the overall governance framework.

There are several legal obligations placed upon the Trust for the use and security of personal data. It is therefore of paramount importance to ensure that information is secure, accurate, available, efficiently managed. Appropriate policies and procedures must be in place and that staff are effectively trained to understand their responsibility for it.

This Information Governance Policy, supported by management accountability and structures sets out the Trust's robust governance framework for information within the organisation.

The vehicle for assessing and reporting Information Governance (IG) in the NHS is the Cyber Assessment Framework (CAF) aligned Data Security and Protection Toolkit (DSPT).

This policy covers:

- All information used by the Trust
- All information systems managed by the Trust
- Any individual using information 'owned' by the Trust
- Any individual requiring access to information 'owned' by the Trust

There are 4 key interlinked strands to the Information Governance Framework:

- Legal Compliance including Confidentiality and Data Protection
- Information Security
- Openness, including Freedom of Information
- Data Quality Assurance

2 Purpose and Outcomes

The purpose of this policy is to ensure that the Trust develops and implements all necessary Information Governance Requirements, as outlined in the CAF aligned DSPT and National Data Guardian Standards.

The outcome of the implementation of the policy is compliance with legal requirements and with the DSPT.

3 Definitions

The 'Trust'	Refers to University Hospitals of Derby and Burton NHS Foundation Trust.
Information Governance	A term used to refer to the work programme encompassing various initiatives namely Data Protection, Freedom of Information, Caldicott, the NHS Confidentiality Code of Practice, Information Security Management/BS799, Records Management and Information Quality Assurance.

Information Asset	An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited efficiently. Information assets can be in a range of formats, for example care records in a filing cabinet, care records on planning software, employee training records, etc.
Information Asset Owners (IAO)	The Information Asset Owner (IAO) will be a senior member of staff who is the nominated owner for one or more identified information assets of the organisation and be responsible for ensuring they are handled and managed
Information Asset Administrators (IAA)	The Information Asset Owner (IAA) is responsible for providing support to the IAO by ensuring policies and procedures are followed, recognise actual or potential security incidents, consult their IAO on incident management, and ensure that information asset registers are accurate and up to date.
Information Governance Leads	The IAA's within each Business Unit will also undertake the role of IG Lead. They are responsible for monitoring divisional compliance against the CAF aligned DSPT and audit requirements. They will attend the bi-monthly Trust Information Governance Group (TIGG) and ensure all relevant information is relayed back to appropriate staff within their unit. The Trust is required to maintain a Register of Processing Activities (ROPA). The nominated IG Lead will be responsible for updating/maintaining a log of data flows for their area.
Serious IG Incident	Any incident involving the actual or potential loss of personal data that could lead to identity fraud or have other significant impact on individuals should be considered as serious.

4 Key Responsibilities/Duties

Groups

4.1 Trust Board

The Trust Board is ultimately responsible for Information Governance within the organisation and is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

4.2 Information Governance Cyber Security and Disaster Recovery Group (IGCSDR)

The Information Governance Cyber Security and Disaster Recovery Group is responsible for steering and overseeing the Trust's IG compliance, including the National Data Guardian Standards set out in the CAF aligned DSPT and review of performance indicators to measure compliance and progress. The group also recommend approval of the annual report prior to submission of the CAF aligned DSPT.

4.3 Trust Information Governance Group (TIGG)

A Network of IG Leads from all areas of the Trust tasked with embedding IG requirements and guidance. They will meet regularly to discuss, promote and implement improvements to IG practice across the Trust.

Individual Roles

4.4 Chief Executive

The Chief Executive is the Accountable Officer with responsibility for ensuring overall Trust compliance with its statutory obligations.

4.5 Senior Information Risk Owner (SIRO)

The SIRO has overall responsibility delegated from the Chief Executive for ensuring that effective
systems and processes are in place to deliver the Information Governance agenda. The SIRO may
appoint a Deputy SIRO.

The SIRO is responsible for:

- Taking ownership of information risk across the Trust.
- Acting as advocate for information risk on the Board and provides written advice to the Accounting Officer on the content of their Statement of Internal Control regarding information risk.
- Advising the Board on the effectiveness of information risk management across the Trust
- Undertaking training as necessary to ensure effectiveness in the role.

4.6 Caldicott Guardian

The Caldicott Guardian is responsible for:

- Ensuring the Trust satisfies the highest practical standards for handling patient information.
- Enabling appropriate information-sharing and make decisions on behalf of the Trust following advice on options for lawful and ethical processing of information, particularly in relation to disclosures.
- Representing and championing Information Governance requirements and issues at Board level.
- Overseeing all procedures that relate to the use of patient and service-user information.

The Caldicott Guardian may appoint a Deputy Caldicott Guardian.

4.7 Executive Chief Digital Information Officer

Will have specific responsibility for ensuring that the risk assessment process is managed

across the IM&T and Information Governance and assign appropriate managers to manage or minimise information risk for both operational services and projects.

4.8 Divisional Directors

Divisional Directors are responsible for monitoring Divisional compliance with Information Governance and providing reports to the Information Governance, Cyber Security and Disaster Recovery Group where necessary.

4.9 Head of Information Governance and Data Protection Officer (DPO)

Responsible for:

- Managing the IG agenda across the Trust and advises on compliance with legal obligations
  including Data Protection Act 2018, UK General Data Protection Regulation (GDPR) and
  other relevant data protection/information governance laws/regulations.
- Providing support to the Caldicott Guardian and Senior Information Risk Owner for Information Governance related issues.
- Completion of the annual CAF aligned DSPT online assessment and its subsequent submission to NHS England to ensure all required evidence is available to demonstrate
  the Trust has achieved the required CAF aligned DSPT standards.
- Monitoring compliance with relevant laws, and internal data protection policies, including
  managing internal data protection activities including Data Protection Impact Assessments
  (DPIAs).
- Cooperating with the supervisory authority and being the first point of contact for supervisory authorities and for individuals whose data is processed.

4.10 Deputy Head of Information Governance

Responsible for:

- Deputising for the Head of Information Governance
- Administration around DPIAs, complaints, meetings, and CAF aligned DSPT evidence
- Supporting the IG incident management process
- Fulfilling IG Officer functions

4.11 Information Asset Owners (IAO)

IAO's will:

- Support the SIRO in their overall information risk management function.
- Take ownership of their Information Asset/s, know what information is associated with the Asset/s and understand the nature and justification of information flows to

and from their Asset/s.
- Review arrangements for assuring the quality of the data that is entered into their Asset/s and detail any concerns they have in relation to data quality.
- Review and update System Specific Security Policies (SSSPs) on an annual basis
- Via IGCSDR, provide an annual report to the SIRO, giving details of any risks that need escalating or giving assurance that there are no risks the SIRO should be made aware of, including the reasons for making this decision.

4.12 IG Leads

IG Leads (previously called Information Assessment Administrators) will:

- Provide support to their IAO's to ensure appropriate policy and procedure is followed and to identify potential or actual risks/incidents to ensure records, including the Information Asset Registers, are accurate and up to date.
- Act as the nominated lead for the division and/or business unit at the TIGG.
- Monitor divisional compliance against IG and CAF aligned DSPT requirements and implement best practice initiatives.
- Maintain and update a log of all information flows and processing activities for their business unit.
- Monitor IG related Datix incidents and take appropriate action with the advice and support from the IG team.
- Attend TIGG meetings and ensure relevant information is relayed back to the appropriate staff within their business unit.

4.13 Clinical Governance Facilitators (CFGs)

The Clinical Governance Facilitator for each division will be responsible for ensuring IG involvement when there are incidents involving breaches of confidentiality. Any such Learning from Patient Safety Events (LFPSE) must have Information Governance representation.

4.14 Information Governance Officer

The IG Officer is responsible for:

- Developing and delivering mandatory training and awareness sessions in relation to Information Governance and the Data Protection Act.
- Providing advice and guidance to all staff on all aspects of Information Governance.
- Working with IG Leads within directorates to ensure consistency and compliance with policy and procedure.

4.15 Subject Access Request Team

Responsible for planning and coordinating a wide range of information access issues to ensure compliance with the Data Protection Act.

4.16 Freedom of Information Manager

Responsible for planning and coordinating a wide range of freedom of information access

issues to ensure compliance with the Freedom of Information Act.

4.17Staff responsible for initiating new projects or changes to Procedures

Responsible for ensuring that the IG Team is involved in the planning stage of all projects to address any IG or privacy issues and to undertake a Data Protection Impact Assessment (DPIA).

4.18 Managers

Managers are responsible for ensuring this policy and all IG requirements are built into local processes. They are also responsible for ensuring staff update their mandatory IG training annually and that any staff working from home are aware of and compliant with the Hybrid Working Guidance/Working from Home IG rules, which are among the IG policies, procedures and guidelines available on neti.

4.19 Trust Staff and contractors (including third party contractors)

All staff and contractors must:

- Be aware of their responsibilities.
- Comply with policies and procedures issued by the Trust including IG documentation available at https://neti.uhdb.nhs.uk/az-nc-ig-sops.
- Comply with Data Protection laws.
- Work within the principles outlined in the Information Governance Framework.
- Update their mandatory IG training on an annual basis.
- Ensure each Information Governance incident is reported through DatixIQ, and escalate serious incidents to the IG team.

5 The Information Governance Framework

The Trust recognises the need for an appropriate balance between openness and confidentiality in the management and use of information.

The Trust will follow the Caldicott principles:

1. Justify the purpose(s) for using confidential information
Every proposed use or transfer of confidential information should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

2. Use confidential information only when it is necessary
Confidential information should not be included unless it is necessary for the specified purpose(s) for which the information is used or accessed. The need to identify individuals should be considered at each stage of satisfying the purpose(s) and alternatives used where possible.

3. Use the minimum necessary confidential information
Where use of confidential information is considered to be necessary, each item of information must be justified so that the minimum amount of confidential information is included as necessary for a given function.

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

5. Everyone with access to confidential information should be aware of their responsibilities Action should be taken to ensure that all those handling confidential information understand their responsibilities and obligations to respect the confidentiality of patient and service users.

6. Comply with the law
Every use of confidential information must be lawful. All those handling confidential information are responsible for ensuring that their use of and access to that information complies with legal requirements set out in statute and under the common law.

7. The duty to share information for individual care is as important as the duty to protect patient confidentiality
Health and social care professionals should have the confidence to share confidential information to care for in the best interests of patients and service users within this 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.

5.1 Data sharing

The Trust recognises the need to share patient information with other health organisations and agencies in a controlled manner consistent with the interests of the patient and, in some circumstances, public interest.

Patients and service users will be informed how their information may be used, who will have access to it, who it will be shared with and the organisations it may be disclosed to. The Trust will publish this through Privacy Notices, leaflets, and posters.

5.2 Record keeping

The Trust fully supports the principles of corporate governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard, both personal information and about patients and staff and commercially sensitive information.

The Trust believes that accurate, timely and relevant information is essential to deliver the highest quality health care. As such it is the responsibility of all clinicians and managers to ensure and promote the quality of information and to actively use information in decision-making processes. The Trust has established and maintains policies and procedures for the management of information.

The Trust will ensure that all Information Assets and transfers/flows of information, into and out of the organisation are adequately protected. Risk assessments must be undertaken annually, taking into consideration the sensitivity of the information. Any medium/high risks identified must be escalated to the SIRO for discussion at the IGCSDR Group. Where there are no risks for escalation the SIRO must be given evidence of security measures in place to provide this assurance.

The Trust will ensure that a Data Protection Impact Assessment (DPIA) is completed for all new projects or changes to practice that involve the processing of personal data. DPIAs that highlight high volumes of personal data or high-risk processes must be sent to the Information Commissioner's Office (ICO) for final sign off.

5.3 Breaches of this policy

In situations where the policy has been breached, appropriate action will be taken in accordance with the Trust's Disciplinary Policy and Procedures with appropriate officers appointed to investigate.

IG incidents or potential incidents that relate to data loss or unauthorised disclosure will be rated depending on the sensitivity of the information and how many individuals are involved. Incidents will be reported, through DatixIQ, in accordance with the Trust's Incident Reporting Procedures and will be monitored and investigated as necessary.

For incidents where there is likelihood that harm may occur, the incident must be reported to the Department of Health and the Information Commissioner's Office (ICO) through the Report an Incident function via the CAF aligned DSPT.

Key Elements of the Information Governance Framework are:

5.4 Openness

- Non-confidential information on the Trust and its services should be available to the public through a variety of media, in line with the Trust's code of openness.
- The Trust has established and will maintain policies to ensure compliance with the Freedom of Information Act.
- The Trust will undertake or commission annual assessments and audits of its policies and arrangements for openness.
- Patients should have ready access to information relating to their own health care, their options for treatment and their rights as patients.
- The Trust have clear procedures and arrangements for liaison with the press and broadcasting media.
- The Trust have clear procedures and arrangements for handling queries from patients and the public.
- Staff have ready access to Information Governance Policies, Procedures and Guidelines including on this intranet page: https://neti.uhdb.nhs.uk/az-nc-ig-sops

5.5 Legal Compliance

- The Trust regards all personal data about patients as confidential.
- The Trust will undertake or commission annual assessments and audits of its compliance with legal requirements.
- The Trust regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise.
- The Trust have established and will maintain policies to ensure compliance with the Data Protection legislation, Human Rights law and the common law duty of confidentiality.
- The Trust will establish and maintain policies for the controlled and appropriate sharing of patient information with other agencies, taking account of relevant legislation.

5.6 Information Security

- The Trust have established and will maintain an Information Asset Register/Record of Processing Activities (ROPA) identifying Information Asset Owners, who are responsible for the identification of risks associated with their asset. The Trust have established and will maintain policies and procedures for the effective and secure management of its policies for its information assets and resources.
- The Trust will undertake or commission annual assessments and audits of its information and its Information Technology (IT) security arrangements.

- All Information Asset Owners and Digital and Data Services will undertake a System Specific Security Policy (SSSP) and risk assessments annually for all Information Assets. They are responsible for escalating to the SIRO, via the IGCSDR Group, any risks that they need to be aware of, or providing assurance that there are no risks for escalation, along with evidence of what this decision has been based on.
- The Trust will promote effective confidentiality and security practice to its staff through policies, procedures and training.

5.7 Data Quality Assurance

- The Trust has established and will maintain policies and procedures for information quality assurance and the effective management of records.
- The Trust will undertake or commission annual assessments and audits of its information quality and records management arrangements.
- Managers are expected to take ownership of, and seek to improve, the quality of information within their services.
- Where possible, information quality should be assured at the point of collection.
- Data standards will be set through clear and consistent definition of data items, in accordance with national standards.
- The Trust will promote information quality and effective records management through policies, procedures/user manuals and training.

5.8 The Cyber Assessment Framework (CAF) aligned Data Security & Protection Toolkit (DSPT)

The CAF aligned DSPT is an online self-assessment tool that provides a systemic and comprehensive approach to assessing the extent to which cyber and information governance risks to essential functions are being managed. All organisations that have access to NHS patient data, systems and networks must use the CAF aligned DSPT to provide annual assurance that they are ensuring risks are being managed, protecting against cyber-attacks and data breaches, detecting cyber security events, minimising the impact of incidents and using and sharing information appropriately.

The Trust will undertake annual assessments and audits of its information management via the CAF aligned DSPT. This will also ensure compliance requirements.

NHS England provide the CAF aligned DSPT results to the Care Quality Commission (CQC) and this forms part of the cross checking of evidence to support the Trust's registration with CQC.

Failure to achieve full CAF aligned DSPT compliance will affect our business, reputation, and approvals for some research.

A CAF aligned DSPT compliance report will be presented to the Board by the Caldicott Guardian
annually.

5.9 Training and Guidance

It is a Department of Health & Social Care and CAF aligned DSPT requirement that all staff

who work within the NHS engage with Information governance and undertake annual training. Failure to do so will result in their access to the Internet being revoked. Managers must ensure that staff refresh on their training annually, via e-learning, watching a Podcast or attending Face-to-Face sessions. Staff in key areas/job roles, i.e. Board members, SIRO, Caldicott Guardian, IG Leads IAOs, IG professionals, must complete additional specialist training.

Further additional training will be developed in response to identified

needs. Specialist advice and guidance is available to all staff from the

IG team.

6 Monitoring Compliance and Effectiveness

Monitoring Requirement	Method	Prepared by	Sent to	Frequency
Freedom of Information	Template containing a summary report of compliance levels	Service Managers	IGCSDR Group	Every other meeting
Clinical Coding	Template containing a summary report of compliance levels	Service Managers	IGCSDR Group	Every other meeting
Subject Access Requests	Template containing a summary report of compliance levels	Service Managers	IGCSDR Group	Every other meeting
Data Quality	Template containing a summary report of compliance levels	Service Managers	IGCSDR Group	Every other meeting
Cyber Security	Template covering recent activities	Director of Digital Head of IG	IGCSDR Group	Every meeting
IG Update (including Incident Management, Records Management)	Template covering recent activities	Head of IG	IGCSDR Group	Every meeting
Risk Register	Template covering recent activities	Head of IG	IGCSDR Group	Twice yearly
Caldicott Report	Report	Head of IG	Trust Board	Annual
CAF aligned DSPT Report	Annual compliance with the CAF aligned DSPT and any outstanding issues	Auditors	IGCSDR Group & Trust Board	Twice yearly to IGCSDR Group, Yearly to Trust Board