Public – To be published on the Trust external website

Information Governance Policy

CORP-0006-v9

Status: Ratified
Document type: Policy

Contents

1. Introduction

Tees, Esk and Wear Valleys NHS Foundation Trust (the Trust) recognises that reliable information is a vital asset. Information Governance (IG) defines how the Trust handles information, particularly personal and sensitive or special category information about patients, service users, staff and confidential business information.

This policy should be read in conjunction with the Trust's Information Governance Management Handbook. This is available on the Trust-wide shared drive here: T:\Intranet Published Documents\Information Governance\Current

Our Journey To Change sets out why we do what we do, the kind of organisation we want to become and the way we will get there by living our values, all of the time. To achieve this, the Trust has committed to three goals.

This policy supports all three goals of Our Journey To Change.

1.1. Strategic goal 1: To co-create a great experience for patients, carers and families

Engaging patients in their own care can promote increased confidence and willingness to take control of their health, which ultimately can lead to healthier behaviours and improved outcomes. (Turakhia, P and Combs, B; 2017)

UK data protection law (UK GDPR and The Data Protection Act 2018), Freedom of Information Act 2000 and Environmental Information Regulations (2004), which underpin all aspects of IG, give transparency to all aspects of the way that information is processed within the Trust.

Implementing this policy provides assurance to patients, carers, families and staff that when records are created they are part of a system that protects and provides evidence of activities that can be requested.

Importantly, patients, carers and families can be assured that they are part of the process of creating records about their care and that they can easily review and contribute to their records.

1.2. Strategic goal 2: To co-create a great experience for our colleagues

Maintaining good quality records has both immediate and long-term benefits for staff. It can directly benefit them, for example in respect of safety. Records management promotes better communication as well as continuity, consistency, and efficiency, and reinforces professionalism. (Wood, C; 2003)

All staff receive mandatory annual Information Governance awareness training which ensures that all colleagues understand their role around the use and sharing of information that is created or used by them. When staff understand their roles and their duties, they can be confident that the actions that they take are consistent, appropriate and defendable.

1.3. Strategic goal 3: To be a great partner

Information and its governance is a key communication tool and is strategic in assisting the Trust when it works with key partners either to improve services or to jointly care for patients. When we discuss our Privacy Notice with our patients and let them know who we work with and have robust agreements about what is going to be shared, we enable information to support outstanding care and service delivery with our partners.

1.4. Trust values and behaviours

Embedding good IG practice across all areas of the Trust enables us to evidence how we live our values of respect, compassion and responsibility in everything we do.

2. Why we need this policy

The Trust has a legal duty as defined within the UK GDPR, Data Protection Act 2018, Freedom of Information Act 2000 and Environmental Regulations Act 2004 to ensure that there is a robust and accountable framework in place.

2.1. Purpose

The purpose of this policy is to:

- Support the core business of the Trust through a robust and accountable IG framework.
- Provide assurance to the Trust and to individuals that all information is dealt with legally and securely.
- Comply with NHS Digital's Data Security and Protection Toolkit requirements.

2.2. Objectives

The objective of this policy is to provide an IG framework that:

- Supports the provision of high-quality care by promoting the efficient, effective and appropriate use of information.
- Ensures compliance with all current legislation, standards and national guidance relating to managing information.

- Develops support arrangements and provides procedures and training so that staff can fulfil their responsibilities for information confidentiality and integrity to consistently high standards.
- Encourages staff to work closely together to prevent duplication of effort and enable more efficient use of resources.
- Measures and understands performance and manages improvement in a structured and effective way.

3. Scope

3.1. Who this policy applies to

- All employees of the Trust, including temporary and bank staff, locums, contractors and volunteers.

3.2. What this policy applies to

- All information including (but not limited to):
    - Information about patients, service users and other clients
    - Personnel information about staff
    - Organisational and corporate information.

- All aspects of handling information, including (but not limited to):
    - Obtaining, creating, amending and deleting
    - Storing in structured record systems – paper and electronic
    - Sharing, disclosing and moving information – fax, e-mail, post and telephone.

- All information systems purchased, developed and managed by or on behalf of the Trust, whether Trust-wide, locality or service-specific.

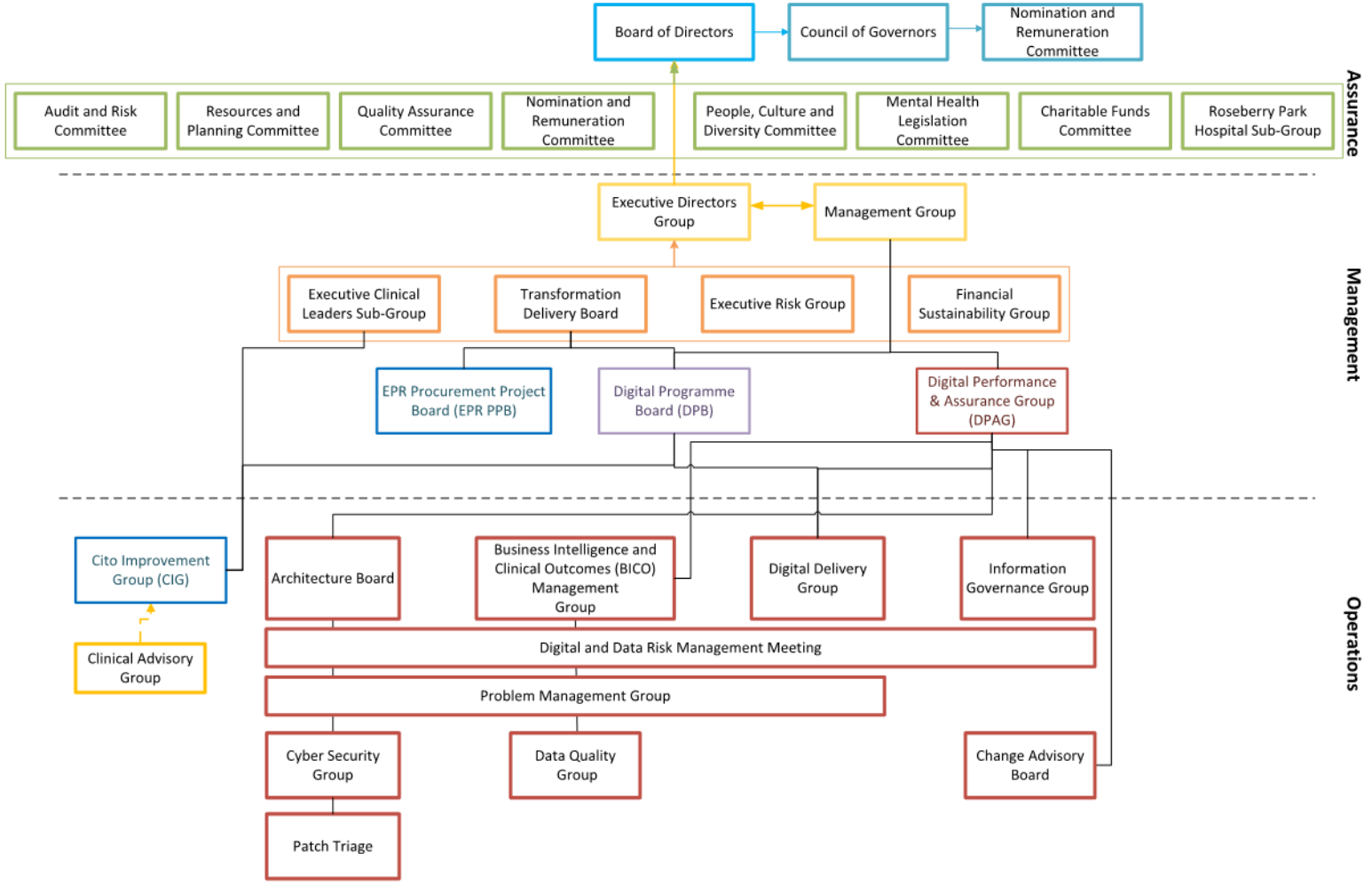
3.3. Roles and responsibilities

Role	Responsibility
Trust Board	• Sponsors of the Trust's IG framework, taking into account legal and NHS requirements. • Ensuring sufficient resources are provided to support the requirements of the policy.
Audit and Risk Committee (ARC)	ARC reviews the establishment and maintenance of an effective system of integrated governance, organisational risk management and internal control to support the achievement of the organisation's Strategic Objectives, and specifically reviews the adequacy of: • the Trust's policies, processes and procedures to manage organisational risk and the internal control framework, including the design, implementation and effectiveness of those systems; • the policies for ensuring compliance with relevant regulatory, legal and code of conduct requirements.
Digital Performance and Assurance Group (DPAG)	• Ensuring processes are in place to address IG issues; develop and maintain policies, standards, procedures and guidance, co-ordinate and raise awareness of IG within the Trust. • Reporting on an exceptions basis to the Executive Directors Group (EDG)) on significant issues, the Terms of Reference of DPAG are given in Appendix 1.
Chief Information Officer - SIRO Executive Medical Director – Caldicott Guardian	• The Board members responsible for championing IG across the Trust; are the Trust's Caldicott Guardian and Senior Information Risk Owner (SIRO). The SIRO is the chair of the DPAG.
Head of Information Governance and Data Protection Officer	• The senior manager responsible for IG and the Trust's nominated Data Protection Officer.

Information Governance team / Information Compliance team	• Coordinate Data Protection activity under UK Data Protection Legislation (UK GDPR and Data Protection Act 2018); • Overseeing the policies and procedures required by Data Protection Legislation and subsequent regulations • Coordinate and review Data Protection Impact Assessments prior to approval at Information Governance Group • Maintaining the Trust's registration with the Information Commissioner's Office • Carrying out compliance checks on the Trust's data usage • Carry out compliance checks against all staff access to personal information on a need-to-know basis • Overseeing the processing of Subject Access Requests • Maintaining the Trust's Data Protection Issues Log • Maintaining the Trust's Subject Access and Disclosure Log and Data Subject Rights Log • Provision of information to staff on the requirements of Data Protection Legislation • Ensuring that any staff with special responsibilities under Data Protection Legislation are kept up to date with developing requirements • Supporting all staff to remain compliant with mandatory Data Security and Protection training • Ensuring that any new systems containing personal data, or new users of existing systems, are introduced in accordance with the Trust's registration as a Data Controller
Director of Corporate Affairs	• Administration of the Freedom of Information Act 2000
Director of Estates and Facilities	• Administration of Environmental Regulations Act 2004
Information Asset Owners (IAOs) and Information Asset Administrators (IAAs)	• IAOs are members of staff senior enough to make decisions concerning a specific information asset at the highest level. • IAOs understands what information is held, added and removed, how information is moved, who has access and why. • IAOs support the SIRO and are central to managing information risk throughout the organisation. • IAAs support IAOs and undertake responsibility for information assets on a day to day basis.
Managers	• On-going compliance by ensuring that the policy and its supporting standards and guidelines relating to IG are built into local processes.

All Trust staff	• Complying with this policy. • Ensuring that they understand their duties and obligations. • Undertaking annual mandatory Data Security and Protection training and any additional awareness relevant to their role.

3.4. Governance Structure

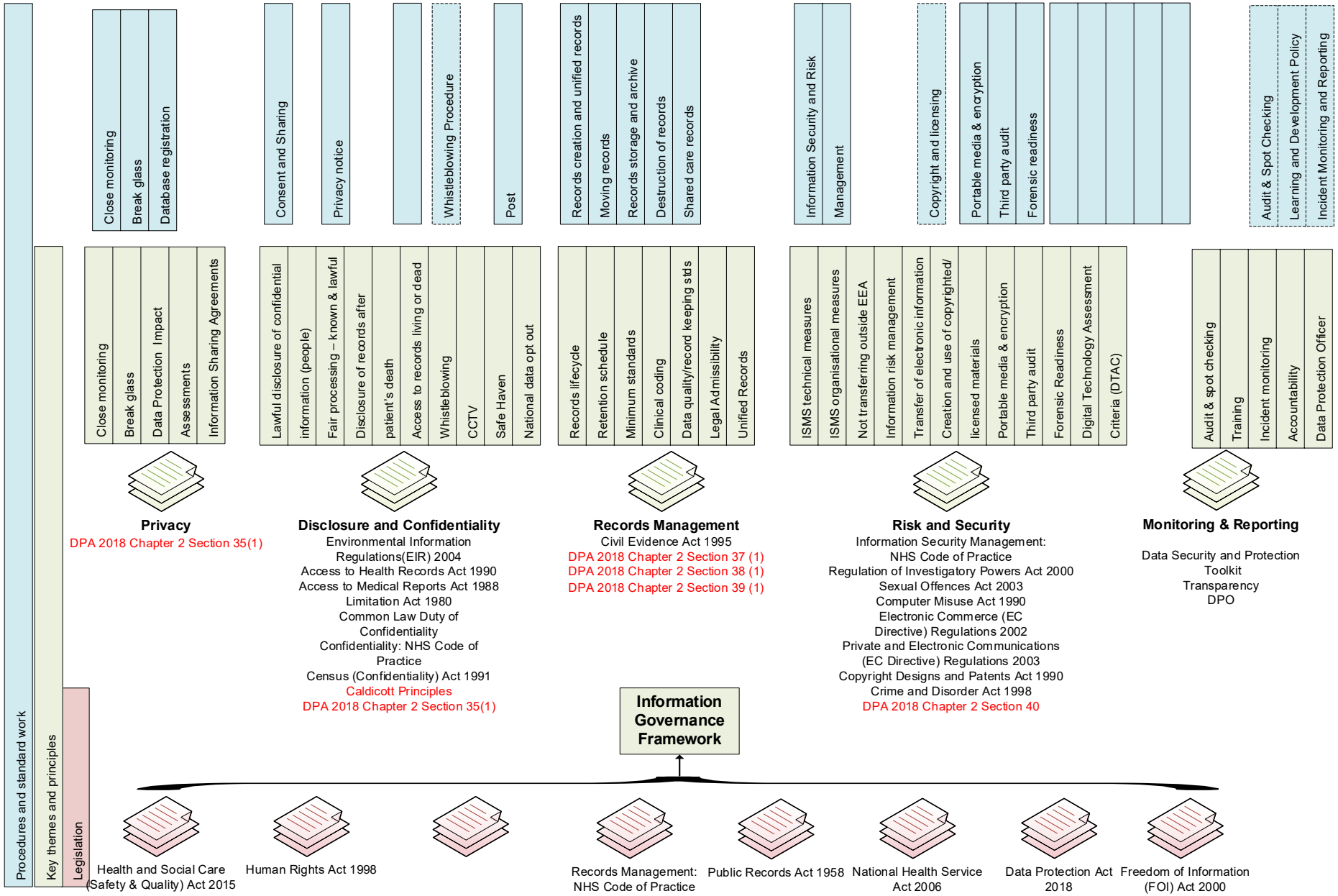


4. Policy

- The Trust recognises the need for balance between openness and confidentiality when managing and using information, and fully supports the principles of corporate governance and public accountability.
- The Trust places equal importance on the confidentiality of, and security arrangements to safeguard, personal information about patients and staff and commercially-sensitive information.
- The Trust is a Data Controller of all systems holding personal identifiable information in use within this organisation and has appointed a Data Protection Officer in line with UK data protection legislation (UK GDPR and Data Protection Act 2018) who maintains a record of all recording and processing activities via its Information Flow and Information Asset registers.
- Accurate, timely, complete, relevant and accessible information is essential to deliver the highest quality health care and inform the decision-making processes.
- Information is constantly being transferred between people, departments and organisations and it is important that appropriate regard is given to security and confidentiality.
- The Trust will identify all major information assets for documentation in an asset register, together with details of the IAO and an assessment of information risk.
- The Trust will uphold the NHS Care Record Guarantee as part of its IG commitment to use records about service users in ways that respect their rights and promote health and well-being. This guarantee covers:
    - People's access to their own records.
    - Control over others' access.
    - How access will be monitored and policed.
    - Options people have to further limit access.
    - Access in an emergency.
    - What happens when someone cannot make decisions for themselves.
- Where there is a need to share patient information with other health organisations or outside agencies, this will be in a controlled and documented manner consistent with the interests and views of the patient or, in rare circumstances, the broader public interest.
- The Trust will establish and maintain policies and procedures to ensure compliance with all relevant legislation including UK GDPR, the Data Protection Act 2018, Human Rights Act 1998 and the common law duty of confidentiality. If staff comply with the provisions of the common law duty of confidence and UK data protection legislation, they will meet the requirements of Article 8 of The Human Rights Act 1998.
- The Trust will develop and maintain information sharing agreements for the controlled, appropriate and lawful sharing of patient information with other agencies, taking account of relevant legislation, current guidance, NHS and professional codes of practice. Action may be taken under the Trust's disciplinary policy and procedure where investigation establishes that an IG breach arose due to a failure to comply with policies and procedures.
- The Trust is committed to a cycle of continuous improvement to continue to meet and exceed the Data Security and Protection Toolkit requirements.
- The Trust will carry out Data Protection Impact Assessments on all Trust systems and processes that involve the use of personal and/or special category data and will report all assessments that indicate high risk to either the individual or the organisation through the DPAG.

5. IG framework

Please see over page.


Procedures and standard work
Key themes and principles
Legislation
Close monitoring
Break glass
Database registration
Consent and Sharing
Privacy notice
Whistleblowing Procedure
Post
Records creation and unified records
Moving records
Records storage and archive
Destruction of records
Shared care records
Information Security and Risk Management
Copyright and licensing
Portable media & encryption
Third party audit
Forensic readiness
Audit & Spot Checking
Learning and Development Policy
Incident Monitoring and Reporting
Close monitoring
Break glass
Data Protection Impact Assessments
Information Sharing Agreements
Lawful disclosure of confidential information (people)
Fair processing – known & lawful
Disclosure of records after patient's death
Access to records living or dead
Whistleblowing
CCTV
Safe Haven
National data opt out
Records lifecycle
Retention schedule
Minimum standards
Clinical coding
Data quality/record keeping stds
Legal Admissibility
Unified Records
ISMS technical measures
ISMS organisational measures
Not transferring outside EEA
Information risk management
Transfer of electronic information
Creation and use of copyrighted/ licensed materials
Portable media & encryption
Third party audit
Forensic Readiness
Digital Technology Assessment Criteria (DTAC)
Audit & spot checking
Training
Incident monitoring
Accountability
Data Protection Officer
Privacy
DPA 2018 Chapter 2 Section 35(1)
Disclosure and Confidentiality
Environmental Information Regulations(EIR) 2004
Access to Health Records Act 1990
Access to Medical Reports Act 1988
Limitation Act 1980
Common Law Duty of Confidentiality
Confidentiality: NHS Code of Practice
Census (Confidentiality) Act 1991
Caldicott Principles
DPA 2018 Chapter 2 Section 35(1)
Records Management
Civil Evidence Act 1995
DPA 2018 Chapter 2 Section 37 (1)
DPA 2018 Chapter 2 Section 38 (1)
DPA 2018 Chapter 2 Section 39 (1)
Risk and Security
Information Security Management: NHS Code of Practice
Regulation of Investigatory Powers Act 2000
Sexual Offences Act 2003
Computer Misuse Act 1990
Electronic Commerce (EC Directive) Regulations 2002
Private and Electronic Communications (EC Directive) Regulations 2003
Copyright Designs and Patents Act 1990
Crime and Disorder Act 1998
DPA 2018 Chapter 2 Section 40
Monitoring & Reporting
Data Security and Protection Toolkit
Transparency
DPO
Information Governance Framework
Health and Social Care (Safety & Quality) Act 2015
Human Rights Act 1998
Records Management: NHS Code of Practice
Public Records Act 1958
National Health Service Act 2006
Data Protection Act 2018
Freedom of Information (FOI) Act 2000

6. Control objectives

6.1. Accountability

No.	Purpose	Legislation/Code of Practice	Policy/Procedure	Evidence for Compliance
6.1.1	The Trust is required to demonstrate that it complies with the principles laid out in the Act	Data Protection Act 2018 Article 5(2)	Data Protection Impact Assessment (DPIA) Procedure Maintenance of Information Systems Policy Introduction or Upgrade of Information Systems Procedure	Policies and Procedures Records of processing activities Data Protection Impact Assessments (DPIA)
6.1.2	The Trust is required to demonstrate transparency regarding processing of personal and special category data - Data Protection by Design		Data Protection Impact Assessment (DPIA) Procedure	Data Minimisation principles (Caldicott) Transparency – privacy notices Co Production of notes with patients Active privacy reporting IGG minutes
6.1.3	The appointment of a Data Protection Officer is seen as an essential role in facilitating accountability	Data Protection Act 2018 Articles 37-39		DPO Appointment – ICO website Reports to Board/SLG regarding compliance Review of DPIA's

6.2. Privacy

No.	Purpose	Legislation/Code of Practice	Policy/Procedure	Evidence for Compliance
6.2.1	Patients and staff must be informed, in general terms, how their information may be used and for what purpose, who will have access to it and the organisations it may be disclosed to.	Data Protection Act (DPA) 2018 Article 5 1(a) Human Rights Act 1998 Article 8 Common law duty of confidentiality	Privacy notice Confidentiality and Sharing Information policy	Record of discussion and issuing of privacy notice on patient's electronic care record Induction checklist
6.2.2	Before implementation of a new or amended system or process involving the use of data, a Data Protection Impact Assessment is carried out to assess privacy risks to individuals in the collection, use and disclosure of information (see also 6.5.4)	Data Protection Act (DPA) 2018 Article 5 1(b) Privacy and Electronic Communications Regulations 2003	Maintenance of Information Systems Policy Information Governance Policy Digital Technology Assessment Criteria (DTAC) Procedure Data Protection Impact Assessment (DPIA) Procedure	Completed Data Protection Impact Assessment and DTAC (see 6.5.4)
6.2.3	Staff who process confidential patient information for purposes beyond care and treatment understand the requirements for compliance with National Data Opt-Out.	NHS England National Data Opt-Out Service	Data Management Policy Research and Development Policy NHS Number Procedure	Use of MeSH system
6.2.4	Patients are informed of their right to opt out of their confidential personal information being used for purposes beyond their care and treatment.	UK GDPR Data Protection Act 2018 NHS England National Data Opt-Out Service	Confidentiality and Sharing Information Privacy Notice	Trust Privacy Notice Evidence of discussing the Trust's Privacy Notice on the electronic patient record
6.2.5	Patients understand which shared care records their confidential personal information is shared into, where to find more information about the	UK GDPR Data Protection Act 2018	Privacy Notice	Trust Privacy Notice

	shared care records and their rights, including the right to opt out.			Evidence of discussing the Trust's Privacy Notice on the electronic patient record

6.3. Disclosure and Confidentiality

No.	Purpose	Legislation/Code of Practice	Policy/Procedure	Evidence for Compliance
6.3.1	The Trust will make non-confidential information about its functions and services available to the public through a variety of media, in line with current legislation and best practice.	Freedom of Information Act 2000 NHS code of openness Environmental Information Regulations (EIR) 2004	Request for Information procedure	FOI Disclosure Request Log Publication Scheme
6.3.2	Patients should have ready access to information relating to their own health care, their options for treatment and their rights as patients. All data subjects are informed of their rights and how to escalate concerns if they are not satisfied with how the Trust is handling their confidential information.	Data Protection Act (DPA) 2018 Article 12-14 Confidentiality: NHS Code of Practice Care Record Guarantee	Request for Information procedure Confidentiality and Sharing Information	Published on external website SAR log Data Protection Officer's job description IG reporting structure Privacy notices published on Trust's external website Patient record evidencing Privacy Notice discussed and shared
6.3.3	The Trust has clear policies and procedures for liaison with the media, and for handling queries and information requests from patients and the public.	Data Protection Act (DPA) 2018 Article 12 Freedom of Information Act 2000	Requests for Information procedure Subject Access SOP Media SOP	Requests for Personal Information log FOI Request Log Complaints/feedback log

			Complaints Policy	
6.3.4	The Trust is committed to implementing the provisions of the Re-use of Public Sector Information Regulations 2015. This provides for an entitlement to re-use information created and held by the Trust subject to certain exemptions and conditions laid down by the legislation. Re-use in this context means using our publicly available information for a purpose different from the one for which it was originally produced, held or disseminated.	Re-use of Public Sector Information Regulations 2005	Requests for Information Procedure	Asset register A published statement of reuse Third-party intellectual property rights register
6.3.5	The Trust regards all identifiable personal information relating to patients as confidential, with disclosure on a strict 'need to know' basis within and outside of the Trust. The Trust has in place a mechanism for recording 'ad hoc' data sharing.	Data Protection Act (DPA) 2018 Article 12	Requests for Information procedure Safeguarding Adults Protocol Safeguarding Children Policy MAPPA Protocol Minimum Standards for Clinical Record Keeping	Close monitoring reporting Privacy officer SOPs and reporting Information sharing agreements MAPPA/MARAC minutes Ad hoc data share requests log (Service Desk Portal)
6.3.6	The Trust regards all identifiable personal information relating to staff as confidential except where national policy requires otherwise.	Data Protection Act (DPA) 2018 Article 12 Terrorism Act 2003	Confidentiality and Sharing information Policy Information Security and Risk Policy	SAR log Information sharing agreements
6.3.7	Staff are trained in the legal framework covering the disclosure of confidential patient information. They are also provided with procedures for obtaining explicit consent and guidance on where to seek advice if they are unsure whether they should disclose such information.	Information Governance Toolkit Data Protection Act (DPA) 2018 Article 5 1(f) Article4 (11) and Article 6 (1)(a)	Confidentiality and Sharing Information Requests for Information procedure Use of Audio and Visual Recordings Procedure	IG Mandatory Training reporting Checklist for consent Data Protection Impact Assessments identifying processes where consent is the

				legal basis for disclosure and their related Standard Operating Procedures
6.3.8	All staff who use patient records are made aware of their responsibility for facilitating and maintaining confidentiality of those records. Systems and processes ensure that employees only have access to those parts of the record required to carry out their role. Access to records is logged and periodically audited.	Common Law Duty of Confidentiality Professional codes of conduct	Confidentiality and Sharing Information policy Records Management Procedures Close Monitoring and Break Glass Standard Operating Processes	Close monitoring and break glass reporting PARIS and network access training record Spot check/audit results Information incident logs and investigations
6.3.9	The Trust has procedures to ensure the ethical obligation to the relatives of the deceased in requiring that confidentiality obligations continue to apply. Records of the deceased are treated as confidential and disclosures only made in line with legislation.	Access to Health Records Act 1990 Common Law Duty of Confidentiality	Access to Health Records Standard Operating Process Request for Information Procedure	Access Request disclosure Log
6.3.10	Deceased patients – A duty of confidentiality remains after a patients' death and so all care must be taken not to disclose information without the correct authority or against the patients known wishes.	Access to Health Records Act 1990	Access to Health Records Standard Operating Process Request for Information Procedure	Access to Health Record Act 1990 disclosure log Caldicott log Data Protection Impact Assessments relevant to processes for sharing information regarding deceased patients
6.3.11	Information given in confidence must not be disclosed unless there is a clear overriding public interest in doing so. What is necessary or proportionate depends on the individual circumstances of each case. The outcome to be achieved in disclosing information must be	Common law duty of confidentiality Data Protection Act (DPA) 2018	Records Management Procedures Confidentiality and Sharing Information policy CPA policy	Access Request disclosure Log Access to Health Record Act 1990 disclosure log

	weighed against the public interest in provision of a confidential health service by the NHS.		Information Security and Risk policy	
6.3.12	The Trust has a documented process for requesting patient-identifiable information for purposes other than direct healthcare including when the requestor does not require the explicit consent of the patient.	Health and Social Care Act 2015 NHS Digital for any exemptions under section 251	Requests for Information procedure Subject Access SOP	Caldicott Log

6.4. Records Management

No.	Purpose	Legislation/Code of Practice	Policy/Procedure	Evidence for Compliance
6.4.1	The Trust will promote information quality assurance and records management through appropriate policies, procedures and training.	Data Protection Act (DPA) 2018 Article 5 1(d)	Records Management Policy Records Management Procedures Data Management Policy Minimum standards for corporate / clinical record keeping	Mandatory Training Report Supervision records
6.4.2	Managers are required to take ownership of, and seek to improve, the quality of information within their services.	Data Protection Act (DPA) 2018 Article 5 1(d)	Records Management Policy Data Management policy	IG Spot Checks Performance reports Audit programmes
6.4.3	Information quality should be assured at the point of collection whenever possible or, as soon as practicable afterwards.		Data Management Policy	Bulk transfer audit trail IG spot checks Data Quality Working Group Terms of Reference, minutes and action log

6.4.4	Data standards will be set through clear and consistent definition of data items, in accordance with national standards.		Data Management Policy Minimum standards for Clinical Record Keeping	Bulk transfer audit trail Integrated Information Centre (IIC) audit trail
6.4.5	Organisations should have processes that address where and how the records of deceased persons are stored.		Records Management Procedures	Archive records log
6.4.6	The Trust has documented processes and procedures to enable the efficient and effective retrieval of such records within legal timescales.	Access to Health Records Act 1990 Data Protection Act (DPA) 2018 (GDPR) Article 5 1(d)	Records Management Procedures Requests for Information procedure	Access request log SAR log Tracking and tracing records
6.4.7	Records, both paper and electronic, are kept within the Trust and our external archives to legally admissible standards. The Trust has processes in place to be able to verify that any computer was not misused and was operating properly at the time a record was produced.	The Civil Evidence Act 1995 The Police and Criminal Evidence (PACE) Act 1984	Records Management Procedures Minimum Standards for Corporate Record Keeping Access to Information Systems policy / procedure	Information Audit Trails Restore contract
6.4.8	Staff are made aware of the Trust's security measures put in place to protect all health records. The Trust has policies and procedures in place to ensure compliance together with disciplinary measures for failure to comply.	The Computer Misuse Act 1990 Data Protection Act (DPA) 2018 Article 5 1(f)	Access to Information Systems policy / procedures Records Management Procedures Disciplinary Policy Close Monitoring and Break Glass standard operating procedures	Audit reports Training records Spot checks ISMS audit Close monitoring and break glass monitoring outputs

6.4.9	The Trust has documented procedures to protect health records during their transportation between sites or organisations.	Data Security and Protection Toolkit	Records Management Procedures Moving records and other sensitive information procedure	Tracking and tracing logs Receipts/postal records Formal contracts and related due diligence (Trust approved transport and external archive)
6.4.10	The Trust ensures that electronic information (patient, staff and business) is held and transferred in accordance with legislation to ensure that confidential information is accessed only by those with a need to know it in order to carry out their role.	The Electronic Communications Act 2000	Incident Reporting and Serious Incident Review Policy Email Policy Encryption Standards Corporate Records Management Guidance System Specific Policies Digital Technologies Assessment Criteria (DTAC) Procedure Access to Information Systems Policy	Audit reports Monitoring reports Incident reports Data Protection Impact Assessments User access audits Role-based access controls
6.4.11	Staff are made aware of the correct procedures to be followed if circumstances arise that require them to breach confidentiality and any policy guidance.	The Public Interest Disclosure Act 1998	Confidentiality and Sharing Information Minimum Standards for Corporate Record Keeping	Disclosure logs Training records Emails/advice log
6.4.12	The Trust adheres to the Department of Health's Records Management Code of Practice regarding: • the management of all NHS record types; • the day-to-day use of NHS records; and	Records Management Code of Practice Retention and disposition schedule Classification scheme	Records Management Procedures	Spot checks Record keeping auditsIG mailbox records

	• minimum retention period schedules for NHS records.			

6.5. Risk and Security

No.	Purpose	Legislation/Code of Practice	Policy/Procedure	Evidence for Compliance
6.5.1	The Trust will promote effective confidentiality and security practices through policies, procedures and training developed to ensure secure management of all information assets.	Data Protection Act (DPA) 2018 (GDPR) Article 5 1(f) Computer Misuse Act 1990 Information Security Management NHS Code of Practice	Information Security and Risk Policy Information Asset Register Procedure	Training reports and attendance records Maintained Information Asset Registers Information Risk Reports SIRO network meetings SIRO communications SIRO/IAO training materials and logs
6.5.2	Potentially affected individuals, the Trust's legal advisers and human resources department are all aware of the possibility of the interception or monitoring of communications or systems usage where this is locally permitted under the provisions of the Regulation of Investigatory Powers Act 2000	Regulation of Investigatory Powers Act 2000 Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (LBPR) Private and Electronic Communications (EC Directive) Regulations 2002	Access to information systems policy / procedure	Induction records Training records
6.5.3	The Trust has processes for protecting its intellectual property, and for ensuring the intellectual property of others is used in accordance with legislation.	Copyright Designs and Patents Act 1990	Intellectual Property Policy Requests for Information procedure	Patent documentation Copyrighted materials

6.5.4	The Digital technology Assessment Criteria for health and social care (DTAC) gives staff, patients and citizens confidence that the digital health tools they use meet our clinical safety, data protection, technical security, interoperability and usability and accessibility standards. The DTAC 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 new digital technologies meet our minimum baseline standards. For developers, it sets out what is expected for entry into the NHS and social care.	Data Protection Act (DPA) 2018, Part 4, Chapter 2 Section 91 which states: *The sixth data protection principle is that personal data must be processed in a manner that includes taking appropriate security measures as regards risks that arise from processing personal data.*	Information Security and Risk Policy DTAC Procedure DTAC Dashboard DTAC minutes DTAC huddle Terms of Reference	Completed DTAC process

6.6. Monitoring and Reporting

No.	Purpose	Legislation/Code of Practice	Policy/Procedure	Evidence for Compliance
6.6.1	The Trust will establish and maintain procedures to monitor and investigate all reported instances of actual or potential data loss or confidentiality breach incidents, details will be included in annual reports.	Data Protection Act (DPA) 2018 (GDPR) Article 5(2) Caldicott Review 2 and 3	Break Glass SOP Information Incidents Procedure (Confidentiality and Privacy Breaches) Incident Recording and Response Policy	Incident reports Action plans Inphase reports Trust Board response re audits IGG monitoring

7. How this policy will be implemented

- Directors, Information Asset Owners and Information Asset Administrators will ensure that this policy is effectively implemented.
- This policy will be published on the Trust's intranet and internet sites and advertised using established communication channels such as e-bulletin, Core Brief and the InTouch news pages.
- Training will be provided at Trust induction and as part of the mandatory and statutory training programme, using Connecting for Health's online IG training tool to deliver mandatory training for staff using a computer at work.
- Regular information governance knowledge and compliance checks will be carried out to assess staff understanding and establish knowledge gaps requiring further training or guidance.
- This policy will be reviewed annually in line with IGT requirements, or more frequently in response to exceptional circumstances, or organisational or legislative changes.

7.1. Implementation action plan

Activity	Expected outcome	Timescale	Responsibility	Means of verification/ measurement
Monitor Mandatory Training compliance	85% staff have passed IG mandatory training	Annual	All Managers	IIC reports

7.2. Training needs analysis

Staff/Professional Group	Type of Training	Duration	Frequency of Training
All Staff	IG Mandatory Training	1.5 hours	Annual
Specialist IG roles	Specific to role	Training-specific	Annual
Information Asset Owners and Administrators	Information Asset Owner (IAO) and Administrator (IAA) training	2 hours	Annual
Senior Information Risk Owner (SIRO)	SIRO training	1 day	Once with annual refresher training
Caldicott Guardian	Caldicott Guardian Training	1 day	Once with annual refresher training
Data Protection Officer	Data Protection Officer training	Exam based qualification	Once with professional obligation to remain up to date with latest developments

8. How the implementation of this policy will be monitored

- The Trust's annual submission to the Cyber Assurance Framework aligned Data Security and Protection Toolkit (DSPT-CAF) is independently audited by Audit One.
- The Trust will undertake or commission annual assessments and audits as part of a programme to monitor the adequacy of this policy and all related policies, procedures and systems.

Number	Auditable Standard/Key Performance Indicators	Frequency/Method/Person Responsible	Where results and any Associate Action Plan will be reported to, implemented and monitored; (this will usually be via the relevant Governance Group).
1	DSP Toolkit	Audit One	DPAG
2	Ad Hoc IG Audits	IT staff when visiting site	Heads of Information and by exception DPAG

9. Definitions

Term	Definition
DSPT-CAF	Cyber Assurance Framework Aligned Data Security and Protection Toolkit - an online system which allows NHS organisations and partners to assess themselves against the NHS England cyber security and information governance standards.
DPIA	Data Protection Impact Assessment
DTAC	Digital Technology Assessment Criteria
ISA	Information Sharing Agreement
SAR	Subject Access Request
Privacy	A state of not being observed or disturbed by other people; being free from public attention
Disclosure	The act of making secret information known
Confidentiality	Maintaining the intention/expectation to keep something secret or private

10. Document control (external)

Date of approval	15 April 2025
Next review date	15 April 2028
This document replaces	CORP-0006-v8 Information Governance Policy
This document was approved	Information Governance Group - 19 February 2025
This document was approved	Digital Performance and Assurance Group - 14 March 2025
This document was ratified by	Management Group
This document was ratified	15 April 2025
An equality analysis was completed on this policy on	16 February 2025
Document type	Public
FOI Clause (Private documents only)	N/A

Change record

Version	Date	Amendment details	Status
	Jul 2015	Incorporated responsibilities under Reuse of Public Sector Information (RoPSI) Regulations 2005 and DP responsibilities following disestablishment of DPA policy (ratified SLG 4/11/15)	Withdrawn
	Jan 2016	The policy underwent a full review and required no changes. Review date extended 3 years.	Withdrawn
	Mar 2018	Reviewed in line with GDPR	Withdrawn
7	Apr 2020	6 month portfolio extension - review date extended to 14 September 2021	Withdrawn
8	16 March 2022	Full revision. Description of how the policy fits with Our Journey To Change added to introduction. Updated onto current policy template with sections 6.1, 6.2 and 7.1 added Minor revision to job titles and governance groups Hyperlinks updated	Withdrawn
9	15 Apr 2025	Full revision with minor amendments throughout to reference latest policies, guidance and terminology Section 6.2 extended to include national data opt out and shared care records Training needs analysis extended to include training needs for job roles with specific responsibility for Information Governance and information risk management. Control objectives for Digital Technical Assessment Criteria strengthened.	Ratified

Appendix 1 - Equality Analysis Screening Form

Section 1	Scope
Name of service area/directorate/department	Finance and Information
Title	Information Governance Policy
Type	Policy
Geographical area covered	Trust-wide
Aims and objectives	• Support the core business of the Trust through a robust and accountable IG framework; • Provide assurance to the Trust and to individuals that all information is dealt with legally and securely. • Comply with NHS Digital NHS Data Security and Protection Toolkit requirements.
Start date of Equality Analysis Screening	01 December 2024
End date of Equality Analysis Screening	16 February 2025

Section 2	Impacts
Who does the Policy, Service, Function, Strategy, Code of practice, Guidance, Project or Business plan benefit?	Trust employees, patients, carers, contractors, volunteers and the organisation as a whole
Will the Policy, Service, Function, Strategy, Code of practice, Guidance, Project or Business plan impact negatively on any of the protected characteristic groups?	• **Race** (including Gypsy and Traveller) **NO** • **Disability** (includes physical, learning, mental health, sensory and medical disabilities) **NO** • **Sex** (Men, women and gender neutral etc.) **NO** • **Gender reassignment** (Transgender and gender identity) **NO** • **Sexual Orientation** (Lesbian, Gay, Bisexual and Heterosexual etc.) **NO** • **Age** (includes, young people, older people – people of all ages) **NO**

	• **Religion or Belief** (includes faith groups, atheism and philosophical beliefs) **NO** • **Pregnancy and Maternity** (includes pregnancy, women who are breastfeeding and women on maternity leave) **NO** • **Marriage and Civil Partnership** (includes opposite and same sex couples who are married or civil partners) **NO**
Describe any negative impacts	None identified
Describe any positive impacts	This policy aims to interpret and pull together the full range of complex law that is intended to keep peoples' information safe and ensure access on a need-to-know basis. The policy also identifies how we evidence that the needs of individuals, both staff and patients, as well the organisational duties are met.

Section 3	**Research and involvement**
What sources of information have you considered? (e.g. legislation, codes of practice, best practice, nice guidelines, CQC reports or feedback etc.)	Feedback from equality bodies, e.g. Care Quality Commission, Disability Rights Commission, etc Research Investigation findings Feedback from equality bodies, e.g. Care Quality Commission, Disability Rights Commission, etc. Health and Social Care Information Centre, Information Commissioners Office, Legislation
Have you engaged or consulted with service users, carers, staff and other stakeholders including people from the protected groups?	Yes
If you answered Yes above, describe the engagement and involvement that has taken place	We have held focus groups with service users and carers regarding the privacy notice and the findings of the Caldicott 2 review. These meetings are held on an Ad Hoc basis as there is information to share or help needed from them. Version 8 of policy underwent full Trust-wide consultation in 2022. The Trust's staff group comprise all protected characteristics.

If you answered No above, describe future plans that you may have to engage and involve people from different groups	

Section 4	**Training needs**
As part of this equality analysis have any training needs/service needs been identified?	No
Describe any training needs for Trust staff	N/A
Describe any training needs for patients	N/A
Describe any training needs for contractors or other outside agencies	N/A

Check the information you have provided and ensure additional evidence can be provided if asked

Appendix 2 – Approval checklist

To be completed by lead and attached to any document which guides practice when submitted to the appropriate committee/group for consideration and approval.

	Title of document being reviewed:	Yes/No/ Not applicable	Comments
1.	**Title**		
	Is the title clear and unambiguous?	Yes	
	Is it clear whether the document is a guideline, policy, protocol or standard?	Yes	
2.	**Rationale**		
	Are reasons for development of the document stated?	Yes	
3.	**Development Process**		
	Are people involved in the development identified?	Yes	
	Has relevant expertise has been sought/used?	Yes	
	Is there evidence of consultation with stakeholders and users?	Yes	
	Have any related documents or documents that are impacted by this change been identified and updated?	Yes	
4.	**Content**		
	Is the objective of the document clear?	Yes	
	Is the target population clear and unambiguous?	Yes	
	Are the intended outcomes described?	Yes	
	Are the statements clear and unambiguous?	Yes	
5.	**Evidence Base**		
	Is the type of evidence to support the document identified explicitly?	Yes	Legal and NHS England
	Are key references cited?	Yes	
	Are supporting documents referenced?	Yes	
6.	**Training**		
	Have training needs been considered?	Yes	
	Are training needs included in the document?	Yes	
7.	**Implementation and monitoring**		

	Title of document being reviewed:	Yes/No/ Not applicable	Comments
	Does the document identify how it will be implemented and monitored?	Yes	
8.	**Equality analysis**		
	Has an equality analysis been completed for the document?	Yes	
	Have Equality and Diversity reviewed and approved the equality analysis?	Yes	Approved by E&D 27 Mar 2025
9.	**Approval**		
	Does the document identify which committee/group will approve it?	Yes	
10.	**Publication**		
	Has the policy been reviewed for harm?	Yes	
	Does the document identify whether it is private or public?	Yes	
	If private, does the document identify which clause of the Freedom of Information Act 2000 applies?	N/A	