Tees, Esk and Wear Valleys
NHS Foundation Trust

Information Governance Policy

CORP-0006.v7

Status: Ratified
Document type: Policy

Contents

1. Why we need this policy

Tees, Esk and Wear Valleys NHS Foundation Trust (the Trust) recognises that reliable information is a vital asset for managing individual patients, staff, resources and services.

Information governance (IG) defines how the Trust handles information, particularly personal and sensitive 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.

1.1. 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 Connecting for Health Information Governance Toolkit requirements.

1.2. 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.

2. Scope

2.1. Who and what this policy applies to

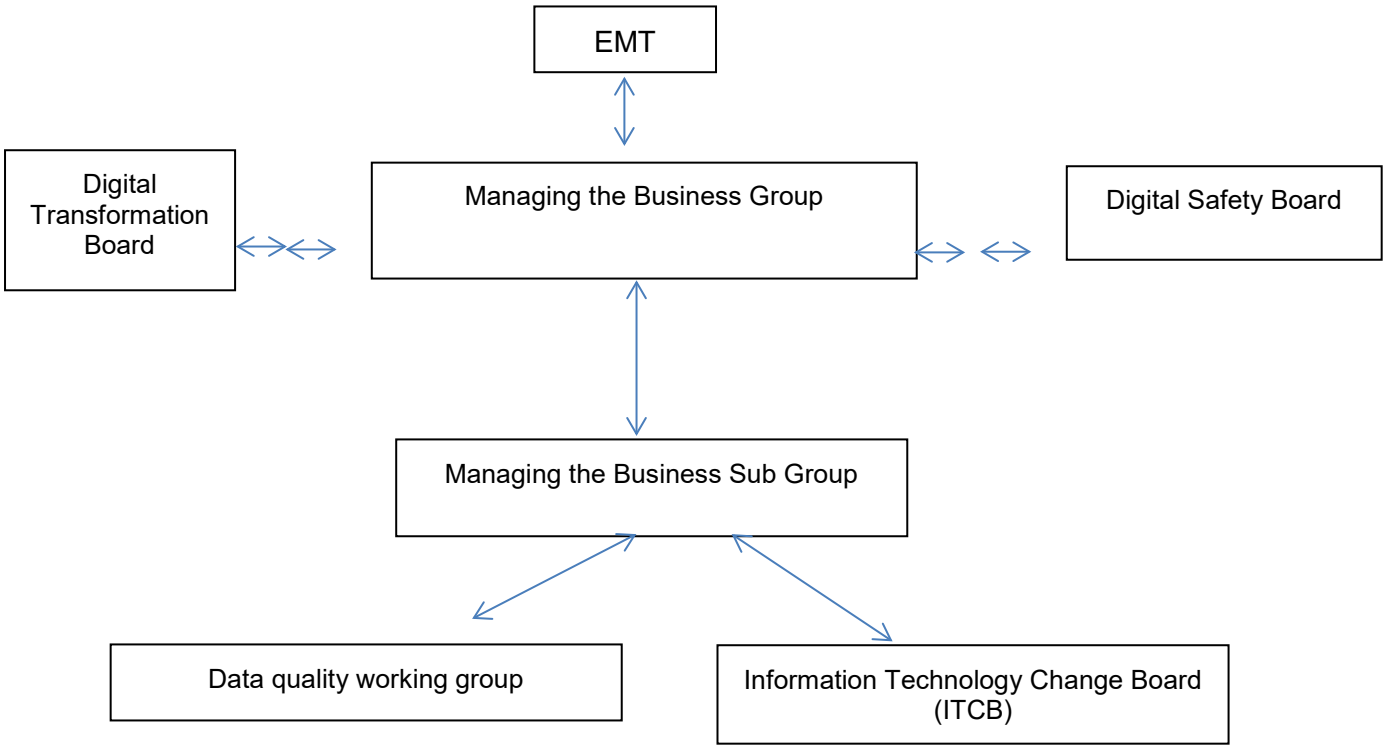
- All employees of the Trust, including temporary and bank staff, locums, contractors and volunteers.
- All information including (but not limited to):
    - Information about patients, service users and other clients;
    - Personnel information about staff;
    - Organisational and corporate information.
- 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.

2.2. 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.
Digital Safety and Information Governance Board (DS&IGB)	• 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 to the Executive Management Team (EMT) on significant issues, the Terms of Reference of DS&IGB are given in Appendix 1.
Executive Director of Finance and Information - SIRO Executive Director of Nursing & Governance – Caldicott Guardian	• The Board members responsible for championing IG across the Trust; as the Trust's Caldicott Guardian and Senior Information Risk Owner (SIRO). The Caldicott Guardian is the chair of the DS&IGB.
Head of Information Governance, Data Protection Officer and Care Programme Approach	• The senior manager responsible for IG and the Trust's nominated Data Protection Officer. •

(CPA)	
Information Governance team	• Coordinate Data Protection activity under Data Protection Act 2018 (GDPR) (DPA); • Overseeing the policies and procedures required by DPA and subsequent regulations • Maintaining the Trust's registration under the Act • Carrying out compliance checks on the trust's data usage • Overseeing the processing of Subject Access Requests • Maintaining the Trust's Data Protection Issues Log • Maintaining the Trust's Subject Access and Disclosure Log • Provision of information to staff on the requirements of the DPA • Ensuring that any staff with special responsibilities under DPA are kept up to date with developing requirements • 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
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 training and awareness relevant to their role.

2.3. Governance structure

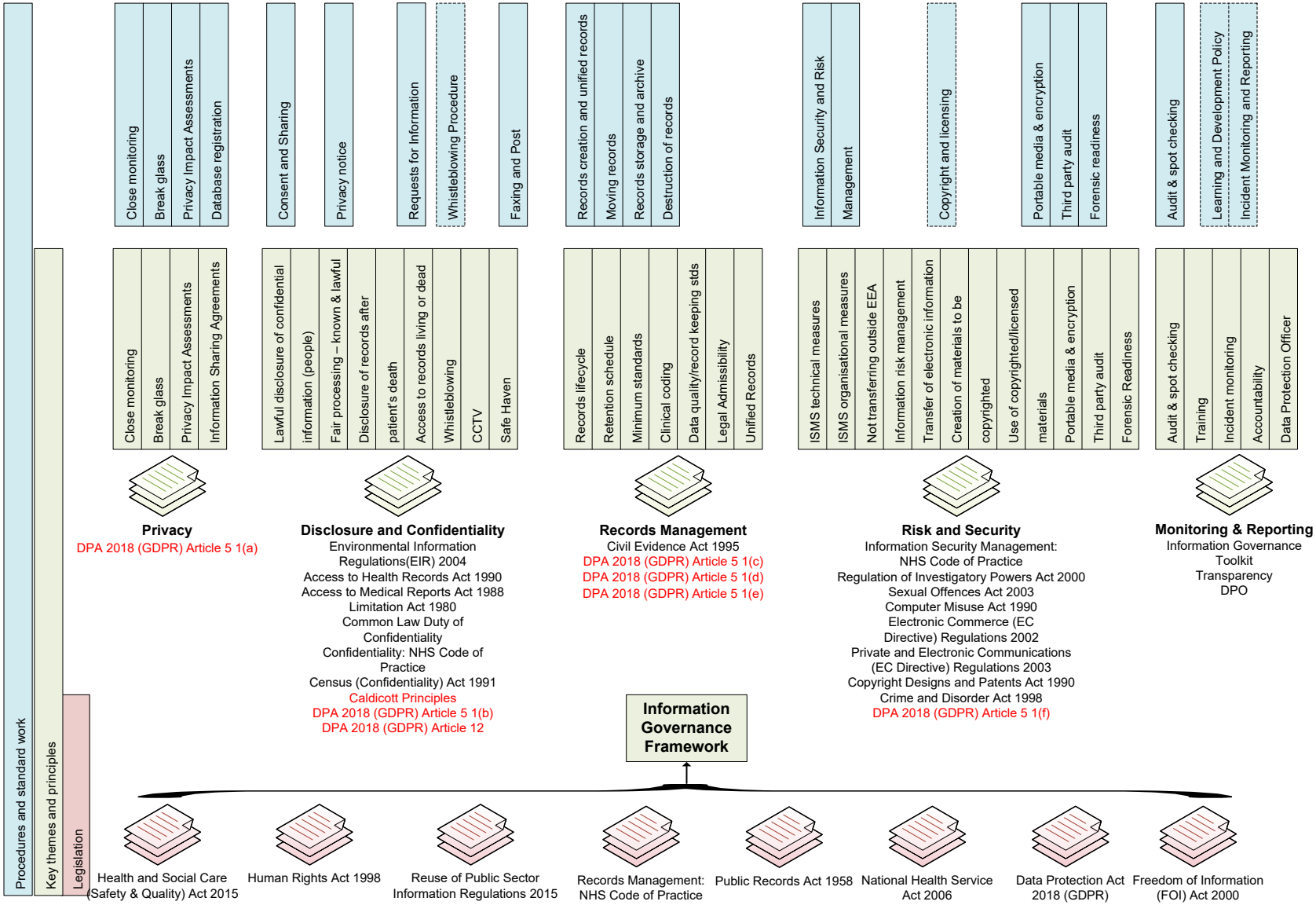


3. Policy

- 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 the new Data Protection Act 2018 (GDPR) legislation 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; and
    - 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 the Data Protection Act 2018 (GDPR), Human Rights Act 1998 and the common law duty of confidentiality.
- 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 Information Governance Toolkit (IGT) requirements.
- If staff comply with the provisions of the common law duty of confidence and the DPA 2018 (GDPR), they will meet the requirements of Article 8 of The Human Rights Act 1998

- The Trust will carry out Data Protection Impact Assessments on all Trust systems and will report all assessments that indicate high risk to either the individual or the organisation through the DS&IGB.

4. IG framework



5. Control objectives

5.1. Accountability

No.	Purpose	Legislation/Code of Practice	Policy/Procedure	Evidence for Compliance
5.1.1	The Trust is required to demonstrate that it complies with the principles laid out in the Act	Data Protect Act 2018 (GDPR) Article 5(2)		Policies and Procedures Records of processing activities Data Protection Impact Assessments (DPIA)
5.1.2	The Trust is required to demonstrate greater transparency - Data Protection by Design			Data Minimisation principles (caldicott) Transparency – privacy notices Co Production of notes with patients Active privacy reporting
5.1.3	The appointment of a Data Protection Officer is seen as an essential role in facilitating accountability	Data Protect Act 2018 (GDPR) Articles 37-39		DPO Appointment Reports to Board/EMT regarding compliance Review of DPIA's

5.2. Privacy

No.	Purpose	Legislation/Code of Practice	Policy/Procedure	Evidence for Compliance
5.2.1	Patients and staff must be informed, in general terms, how their information may be used and	Data Protection Act (DPA) 2018 (GDPR) Article 5 1(a)	Privacy notice Confidentiality and	Record of discussion and issuing of privacy

	for what purpose, who will have access to it and the organisations it may be disclosed to.	Human Rights Act 1998 Article 8 Common law duty of confidence	Sharing Information policy	notice on patient's electronic care record Induction checklist
5.2.2	Before a project begins, a Privacy Impact Assessment is carried out to assess privacy risks to individuals in the collection, use and disclosure of information	Data Protection Act (DPA) 2018 (GDPR) Article 5 1(b) Privacy and Electronic Communications Regulations 2003	Project Management Framework Maintenance of Information Systems Policy Information governance policy	Completed Privacy Impact Assessment

5.3. Disclosure and Confidentiality

No.	Purpose	Legislation/Code of Practice	Policy/Procedure	Evidence for Compliance
5.3.1	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 Request Log Publication Scheme
5.3.2	Patients should have ready access to information relating to their own health care, their options for treatment and their rights as patients.	Data Protection Act (DPA) 2018 (GDPR) Article 12 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
5.3.3	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 (GDPR) Article 12 Freedom of Information Act	Requests for Information procedure Subject Access SOP Media SOP	SAR log FOI Request Log

		2000		
5.3.4	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 publically 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
5.3.5	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.	Data Protection Act (DPA) 2018 (GDPR) Article 12	Requests for Information procedure Safeguarding Adults Protocol Safeguarding Children Policy MAPPA Protocol	Close monitoring reporting Privacy officer SOPs and reporting Information sharing agreements MAPPA/MARAC minutes
5.3.6	The Trust regards all identifiable personal information relating to staff as confidential except where national policy requires otherwise.	Data Protection Act (DPA) 2018 (GDPR) Article 12 Terrorism Act 1994	Confidentiality and Sharing information Policy Information Security and Risk Policy	SAR log Information sharing agreements
5.3.7	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 (GDPR) Article 5 1(f) Article4 (11) and Article 6 (1)(a)	Confidentiality and Sharing Information Requests for Information procedure	IG Mandatory Training reporting Checklist for consent
5.3.8	All staff who use patient records are made aware of their responsibility for facilitating and	Common Law Duty of	Confidentiality and	Close monitoring 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.	Confidentiality Professional codes of conduct	Sharing Information policy Records Management Procedures Close Monitoring and Break Glass Standard Operating Processes	break glass reporting PARIS and network access training record Spot check/audit results
5.3.9	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
5.3.10	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
5.3.11	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 weighed against the public interest in provision of a confidential health service by the NHS.	Common law duty of confidence Data Protection Act 1998	Records Management Procedures Confidentiality and Sharing Information policy CPA policy Information Security and Risk policy	Access Request disclosure Log Access to Health Record Act 1990 disclosure log
5.3.12	The Trust has a documented process to inform anyone requesting patient-identifiable information for purposes other than direct healthcare of the need to gain approval from PIAG, unless they have 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

5.4. Records Management

No.	Purpose	Legislation/Code of Practice	Policy/Procedure	Evidence for Compliance
5.4.1	The Trust will promote information quality assurance and records management through appropriate policies, procedures and training.	Data Protection Act (DPA) 2018 (GDPR) 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
5.4.2	Managers are required to take ownership of, and seek to improve, the quality of information within their services.	Data Protection Act (DPA) 2018 (GDPR) Article 5 1(d)	Records Management Policy Data Management policy	IG Spot Checks Performance reports Audit programmes
5.4.3	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
5.4.4	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 IIC audit trail
5.4.5	Organisations should have processes that address where and how the records of deceased persons are stored.		Records Management Procedures	Archive records log
5.4.6	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

5.4.7	Records, both paper and electronic, are kept within the Trust 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 Corporate Records Management Guidance Access to Information Systems policy / procedure	Information Audit Trails
5.4.8	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 (GDPR) Article 5 1(f)	Access to Information Systems policy / procedures Records Management Procedures Disciplinary Policy	Audit reports Training records Spot checks ISMS audit
5.4.9	The Trust has documented procedures to protect health records during their transportation between sites or organisations.	Information Governance Toolkit	Records Management Procedures Moving records and other sensitive information procedure	Tracking and tracing logs Receipts/postal records
5.4.10	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 Investigating Policy Encryption Standards Corporate Records Management Guidance System Specific Policies	Audit reports Monitoring reports Incident reports
5.4.11	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 Corporate Records Management Guidance	Disclosure logs Training records Emails/advice log
5.4.12	The Trust adheres to the Department of Health's Records Management Code of Practice regarding:	Records Management Code of Practice Retention and disposition	Records Management Procedures	Spot checks Record keeping audits

	• the management of all NHS record types; • the day-to-day use of NHS records; and • minimum retention period schedules for NHS records.	schedule Classification scheme		Ask Abby logs IG mailbox records

5.5. Risk and Security

No.	Purpose	Legislation/Code of Practice	Policy/Procedure	Evidence for Compliance
5.5.1	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
5.5.2	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
5.5.3	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

5.6. Monitoring and Reporting

No.	Purpose	Legislation/Code of Practice	Policy/Procedure	Evidence for Compliance
5.6.1	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 Incident Reporting and Investigating Policy	Incident reports Action plans Datix reports Trust Board response re audits IG monitoring

6. 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. How this policy will be audited

The Trust's annual submission to the IGT is independently audited by Audit North.
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.

8. Definitions

Term	Definition
IGT	Information Governance Toolkit - an online system which allows NHS organisations and partners to assess themselves against the Department of Health information governance standards.
DPIA	Data Protection Impact Assessment
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

9. Document control

Date of approval:	14 March 2018	
Next review date:	14 September 2021	
This document replaces:	CORP-0006-v6 Information Governance Policy	
Lead:	Name	Title
	Louise Eastham	Head of Information Governance, Data Protection Officer and Care Programme Approach (CPA)
Members of working party:	Name	Title
	Theresa Parks Samantha Swales Lynn Holtam Andrea Shotton	Information Governance Manager Privacy Officer Information Security Officer Information Risk, Policy and Records Standards Manager
This document has been agreed and accepted by: (Director)	Name	Title
	Drew Kendall	Director of Finance and Information
This document was approved by:	Name of committee/group	Date
	Digital Safety and Governance Board	07 March 2018
This document was ratified by:	Name of committee/group	Date
	Executive Management Team	14 March 2018
An equality analysis was completed on this document on:	March 2018	
Amendment details:	July 2015 – Incorporated responsibilities under Reuse of Public Sector Information (RoPSI) Regulations 2005 and DP responsibilities following disestablishment of DPA policy (ratified EMT 4/11/15) 11 Jan 2016 – the policy underwent a full review and required no changes. Review date extended 3 years. 14 Mar 2018 – reviewed in line with GDPR 2020 – 6 month portfolio extension - review date extended to 14 September 2021	

Equality Analysis Screening Form

Name of Service area, Directorate/Department i.e. substance misuse, corporate, finance etc	Finance and Information					
Name of responsible person and job title	Louise Eastham Information Governance and Records Manager					
Name of working party, to include any other individuals, agencies or groups involved in this analysis	Information Governance Team, Information Directorate, SIRO network and ISGG					
Title	Information Governance Policy					
Is the area being assessed a	Policy/Strategy	x	Service/Business plan		Project	
	Procedure/Guidance				Code of practice	
	Other – Please state					
Geographical area	Every staff member in the Trust					
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 Connecting for Health Information Governance Toolkit requirements.					
Start date of Equality Analysis Screening	01 March 2018					
End date of Equality Analysis Screening	07 March 2018					

Please read the Equality Analysis Procedure for further information

1. 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					
2. Will the Policy, Service, Function, Strategy, Code of practice, Guidance, Project or Business plan impact negatively on any of the protected characteristic groups below?					
Race (including Gypsy and Traveller)	No	**Disability** (includes physical and mental impairment)	No	**Gender** (Men and women)	No
Gender reassignment (Transgender and gender identity)	No	**Sexual Orientation** (Lesbian, Gay, Bisexual and Heterosexual)	No	**Age** (includes, young people, older people – people of all ages)	No
Religion or Belief (includes faith groups, atheism and some other non religious beliefs - does not include political beliefs	No	**Pregnancy and Maternity** (includes pregnancy women, women who are breastfeeding and women on maternity leave)	No	**Marriage and Civil Partnership** (includes opposite sex and same sex couples who are either married or civil partners)	No
Yes – Please describe the anticipated negative impact **No – Please describe any positive outcomes** 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.					

3. Please indicate the sources of information you have taken into consideration regarding the formulation of this Policy, Service, Function, Strategy, Code of practice, Guidance, Project or Business plan benefit			
Sources of Information			
Department of Health/Care Quality Commission Findings etc		Service user complaints	
Staff grievances		Data collection/Analysis	
Feedback from equality bodies, e.g. Care Quality Commission, Disability Rights Commission, etc	**x**	Feedback from equality bodies, e.g. Care Quality Commission, Disability Rights Commission, etc.	**x**
Research (both internal & external)	**x**	Community Consultation/Consultation Groups	
Investigation findings	**x**	Internal Consultation	
Media		Other (please state) Health and Social Care Information Centre, Information Commissioners Office, Legislation	**x**

4. Have you engaged or consulted with service users, carers, staff and other stakeholders including people from the following protected groups?: Race, Disability, Gender, Gender reassignment (Trans), Sexual Orientation (LGB), Religion or Belief, Age, Pregnancy and Maternity or Marriage and Civil Partnership

Yes – Please 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.

No – Please describe future plans that you may have to engage and involve people from different groups

5. As part of this equality analysis have any training needs/service needs been identified?

No	Please describe the identified training needs/service needs below				
A training need has been identified for					
Trust staff	No	Service users	No	Contractors or other outside agencies	No
Make sure that you have checked the information and that you are comfortable that additional evidence can provided if you are required to do so					
The completed EA has been signed off by: You the Policy owner/manager: Louise Eastham Head of Information Governance, Data Protection and CPA					Date:07 March 2018
Your reporting manager: Drew Kendall Finance and Information Director					Date: 07 March 2018
Please forward this form by email to: tewv.policies@nhs.net **Please Telephone: 0191 3336267/6542 for further advice and information on equality analysis**					