

INFORMATION GOVERNANCE POLICY

POLICY		
Reference	ISP 04	
Approving Body	Information Governance Data Protection and Cyber Security Committee	
Date Approved	January 2026	
For publication to external SFH website	Positive confirmation received from the approving body that the content does not risk the safety of patients or the public:	
	YES	NO
	x	
Issue Date	2026	
Version	10	
Summary of Changes from Previous Version	Updates to Definitions and Abbreviations	
Supersedes	9	
Document Category	Information Governance	
Consultation Undertaken	Information Governance Working Group	
Date of Completion of Equality Impact Assessment	December 2025	
Date of Environmental Impact Assessment (if applicable)	Not applicable	
Legal and/or Accreditation Implications	Failure to undertake could result in enforcement action UK General Data Protection Regulation Computer Misuse Act 1990	
Target Audience	All staff	
Review Date	2 years	
Sponsor (Position)	Director of Corporate Affairs	
Author (Position & Name)	Head of Data Security and Privacy	
Lead Division/ Directorate	Corporate	
Lead Specialty/ Service/ Department	Information Governance	
Position of Person able to provide Further Guidance/Information	Head of Data Security and Privacy Information Governance Team	

Associated Documents/ Information	Date Associated Documents/ Information was reviewed
Not Applicable.	
Template control	April 2024

This information can be made available in alternative formats, such as easy read or large print, and may be available in alternative languages, upon request. Please contact sfh-tr.information.governance@nhs.net.

Contents

1.0 INTRODUCTION	4
2.0 POLICY STATEMENT.....	5
3.0 DEFINITIONS/ ABBREVIATIONS	5
4.0 ROLES AND RESPONSIBILITIES	9
5.0 APPROVAL.....	11
6.0 DOCUMENT REQUIREMENTS	11
6.1.1 Openness.....	11
6.1.2 Legal Compliance	11
6.1.3 Information Security	12
6.1.4 Quality Assurance.....	13
7.0 MONITORING COMPLIANCE AND EFFECTIVENESS	14
8.0 TRAINING AND IMPLEMENTATION.....	15
9.0 IMPACT ASSESSMENTS	15
10.0 EVIDENCE BASE (Relevant Legislation/ National Guidance) AND RELATED SFHFT DOCUMENTS	15
11.0 KEYWORDS.....	16
12.0 APPENDICES	16
APPENDIX 1 - EQUALITY IMPACT ASSESSMENT FORM (EQIA)	17
Appendix 2- List of guidance that has been used to develop this policy.....	19
Appendix 3 - Information Lifecycle Management Strategy.....	22

1.0 INTRODUCTION

Information governance (IG) is all about how to manage and share information appropriately. Information is a vital asset. This document sets out the high-level principles across the community for confidentiality, integrity and availability of information and the role of data security to promote and build a level of consistency across the community on these principles.

1. **Confidentiality** – accessible to those who have a proven need to see it.
2. **Integrity** – information in systems being accurate and up to date.
3. **Availability** – information being there when it is needed to support care.



The formal framework that leaders of all health and social care organisations should commit to is set out in the [National Data Guardian's ten data security standards](#)¹. These are the basis of the [Data Security and Protection Toolkit](#)² that the Trust and other health and social care organisations must use to assess their information governance performance. Under data protection legislation, organisations that process personal data are accountable for, and must be able to demonstrate their compliance with the legislation. The arrangements set out in this and related [policies and procedures](#)³ are intended to achieve this demonstrable compliance.

It is your responsibility to ensure you understand and comply with this policy.

¹ <https://www.gov.uk/government/publications/data-security-and-protection-for-health-and-care-organisations>

² <https://www.dsptoolkit.nhs.uk/>

³ <https://www.sfh-tr.nhs.uk/about-us/regulatory-information/non-clinical-policies/>

Failure by staff to adhere to this policy and all supporting guidance will be considered gross misconduct and **may result in disciplinary action**.

2.0 POLICY STATEMENT

The purpose of this policy is to protect all information assets to a high standard. By promoting a culture of good practice around the processing of confidential information at all levels, the policy aims to ensure that all confidential information held by, or on behalf of the Trust is:

1. held securely and confidentially.
2. obtained fairly and lawfully.
3. protected against unauthorised access.
4. recorded accurately and reliably.
5. used effectively and ethically, and
6. shared and disclosed appropriately and lawfully.

Moreover, all staff must protect the Trust's information assets from all threats, whether internal or external, deliberate or accidental.

The Trust:

- Believe that accurate, timely and relevant information is essential to deliver the highest quality of care.
- Supports the principles of Corporate Governance and recognises its public accountability but equally places importance on the confidentiality and security of both personal information about staff and patients and commercially sensitive information.
- Recognises the need to share confidential patient information with other health and care organisations and other agencies who work in partnership to deliver care and will do so in a controlled manner that is consistent with the interests of the patient, and in some circumstances, the public interest.

3.0 DEFINITIONS/ ABBREVIATIONS

Anonymised Data	Anonymised data refers to personal information that has been modified in such a way that individuals can no longer be identified
Artificial Intelligence (AI)	Artificial intelligence (AI) refers to the ability of computer systems to perform tasks that typically require human intelligence, such as learning, reasoning, decision-making, and problem-solving.
Breach of confidentiality	Is the unauthorised disclosure of confidential information.
Confidential Information	can be anything that relates to deceased and living patients, staff or any other information (such as contracts, tenders etc) held in any form (such as paper or other forms like electronic, microfilm, audio or video)

	howsoever stored (such as patient records, paper diaries, computer or on portable devices such as laptops, PDAs, iPads, mobile telephones) or even passed by word of mouth. Person identifiable information is anything that contains the means to identify an individual. Confidential includes both information 'given in confidence' and 'that which is owed a duty of confidence' and is adapted to include 'sensitive' as defined in the Data Protection Act.
Consent – Explicit and Implied	<p>Explicit consent – If confidential patient information is used for purposes beyond individual care, for example a research project, then it will normally be necessary for staff to obtain explicit consent. This is a very clear and specific statement of consent. It can be given in writing, verbally or through another form of communication such as sign language.</p> <p>Implied consent – If confidential patient information is accessed and used for individual care then consent is implied, without the patient having to explicitly say so. This is because it is reasonable for patients to expect that relevant confidential patient information will be shared with those caring for them on a need-to-know basis.</p>
Data Controller	Sherwood Forest Hospitals NHS Foundation Trust is registered as a Data Controller with the Information Commissioner's Office. A Data Controller is defined as 'a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are or are to be processed'.
Data flow	Data flow within a system describes the path and transformation of data as it moves between components, such as from a source to a process, and then to a storage or destination, with data flow diagrams (DFDs) used to visually map these journeys.
Data Leakage	Data Leakage refers to the potential risk for data being leaked to services and/or unintended audiences.
Data Processor	A processor is a natural or legal person (not an employee), public authority, agency or other body which processes personal data on behalf of the controller. Processors act on behalf of the relevant controller and under their authority. In doing so, they serve the controller's interests rather than their own.
Data Protection Act 2018	The Data Protection Act 2018 controls how your personal information is used by organisations, businesses or the government. The Data Protection Act 2018 ² is the UK's implementation of the General Data Protection Regulation (GDPR).
Data subject	This is the technical term for the individual whom particular personal data is about. In this policy we generally use the term 'patients and staff' instead.
Disclosure	Means the divulging of or provision of access to data.
DUAA	Data (Use and Access) Act 2025 is new UK legislation that updates and modernises data protection law while keeping the core framework of the UK GDPR and Data Protection Act 2018 in place.

Human Rights Act 1998	<p>The Human Rights Act 1998 requires that any intrusion into the private and family life of an individual must be in accordance with the law, proportionate and necessary for:</p> <ul style="list-style-type: none"> • national security • public safety • the economic well-being of the country • for the prevention of disorder or crime for the protection of health or morals or for the protection of the rights and freedoms of others.
ICO (Information Commissioner's Office)	<p>The ICO is the supervisory authority for Data Protection in the UK. They offer advice and guidance, promote good practice, monitor breach reports, conduct audits and advisory visits, consider complaints, monitor compliance and take enforcement action where appropriate.</p>
Identifiable living individual	<p>Means a living individual who can be identified, directly or indirectly, by reference to –</p> <p>(a) An identifier such as a name, an identification number, location data or an online identifier, or</p> <p>(b) One or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identify of the individual.</p>
Information Asset	<p>A body of information that is defined and managed as a single unit, so that it can be understood, protected, used and shared effectively.</p>
Information Asset Administrator (IAA)	<p>Information Asset Administrator. IAAs are operational staff with day-to-day responsibility for managing risks to their information asset(s).</p>
Information Asset Owner (IAO)	<p>Information Asset Owner. IAOs are senior individuals responsible for maintaining good Data Protection and Security/Information Governance arrangements and standards within the relevant business/service areas of the Trust for which they have responsibility.</p>
Information Asset Register (IAR)	<p>Information Asset Register. The Trust's information asset register is stored within CoreStream and populates when completing the DPIA.</p>
Information Processing	<p>Almost anything we do with data counts as processing, including collecting, recording, storing, using, analysing, combining, disclosing, or deleting it.</p>
Machine Learning (ML)	<p>Machine Learning is a type of technology within Artificial Intelligence (AI) that allows computer systems to learn from data. Instead of being programmed with specific instructions, these systems can recognise patterns and make decisions or predictions based on new information.</p>
Personal data³	<p>Personal data means information about a particular living individual 'data subject'. It does not need to be 'private' information – even information which is public knowledge or is about someone's professional life can be personal data.</p> <p>It does not cover truly anonymous information – but if you could still identify someone from the details, or by combining it with other information, it will still count as personal data.</p>

	<p>It only includes paper records if we plan to put them on a computer (or other digital device) or file them in an organised way. In the Trust, all paper records are technically included – but will be exempt from most of the usual Data Protection rules for unfiled papers and notes.</p> <p>Examples of personal information include:</p> <ul style="list-style-type: none"> • a name • identification number i.e. NHS number, NI number • location data • an online identifier i.e. IP addresses and cookie identifiers • one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Processing	Almost anything we do with data counts as processing, including collecting, recording, storing, using, analysing, combining, disclosing or deleting it.
Pseudonymised Data	Pseudonymised data refers to personal information from which direct identifiers have been removed or replaced with artificial substitutes, such as a reference number. This means the data cannot be linked to a specific individual without access to additional, separate information.
Public Interest	Under common law, staff are permitted to disclose personal information in order to prevent and support detection, investigation and punishment of serious crime and/or to prevent abuse or serious harm to others where they judge, on a case by case basis, that the public good that would be achieved by the disclosure outweighs both the obligation of confidentiality to the individual patient concerned and the broader public interest in the provision of a confidential service. Another example would be in response to a Pandemic.
Special categories of personal data	<p>The special categories of personal data are:</p> <ol style="list-style-type: none"> racial or ethnic origin political opinions religious or philosophical beliefs trade-union membership genetic data, biometric data for the purpose of uniquely identifying a natural person data concerning health data concerning a natural person's sex life or sexual orientation.
Staff	Means all staff (including Medirect, Skanska, agency and contractor colleagues)
Third Party	Any person, agency/organisation authorised by the data controller to process data for a specified purpose on their behalf.
Trust	Refers to Sherwood Forest Hospitals NHS Foundation Trust
UK GDPR	In the UK, data protection is governed by the UK General Data Protection (UK GDPR)

4.0 ROLES AND RESPONSIBILITIES

Chief Executive

The Chief Executive has overall responsibility for this policy within the Trust. Implementation of, and compliance with this policy is delegated to the Senior Information Risk Owner (SIRO), Caldicott Guardian, Data Protection Officer (DPO), and members of the Data Protection and Cyber Security Committee.

Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner (SIRO) is responsible to the Chief Executive for Information Governance, who takes ownership of the Trust's information risk policy, acts as an advocate for information risk on the Board and provides written advice to the Chief Executive on the content of the Statement of Internal Control in regard to information risk. The SIRO also reports annually to the Trust Board on Information Governance performance.

Caldicott Guardian

The Chief Medical Officer is the 'conscience' of the organisation, providing a focal point for patient confidentiality, information sharing and advising on the options for lawful and ethical processing of information as required.

Data Protection Officer

We are a public authority and have appointed a Data Protection Officer (DPO). The DPO reports to the Senior Information Risk Owner (SIRO) and works with the Caldicott Guardian. The DPO is tasked with monitoring compliance with Data Protection legislation, our data protection policies, awareness-raising, training, and audits. Our DPO acts as a contact point for the Information Commissioner's Office. When performing their tasks, our DPO has due regard to the risk associated with processing operations, and considers the nature, scope, context and purposes of processing.

Information Asset Owners

Information Asset Owners (IAOs) must be senior/responsible individuals involved in running the relevant business. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. As a result, they are able to understand and address risks to the information and ensure that information is fully used within the law for the public good. They provide a written judgement of the security and use of their asset annually to support the audit process. When carrying out a Data Protection Impact Assessment, we seek the advice of our Data Protection Officer who also monitors the process.

Information Asset Administrators (IAAs)

Information Asset Administrators ensure that Information Governance policies and procedures are followed, recognise actual or potential Information Governance security incidents and take

steps to mitigate those risks, consult their Information Asset Owners on incident management, and ensure that information asset registers are accurate and up to date. When carrying out a Data Protection Impact Assessment, we seek the advice of our Data Protection Officer who also monitors the process.

Line Managers

Line managers are responsible for ensuring that all Divisional/ Departmental staff are made aware of the Information Governance policies and procedures and comply with them. They are also responsible for ensuring staff are released to undertake mandatory annual data security awareness training.

Information Governance (data security and privacy) Team

The data security and privacy team will provide expert advice and guidance to all staff on all elements of Information Governance. The team is responsible for:

- Developing, maintaining, and communicating data security policies and procedures
- Working with the Trust and other organisations to establish agreements on how information is to be shared.
- Developing data security awareness and training programs for staff ensuring compliance with Data Protection, Information Security, and other relevant legislation
- Providing support to the Caldicott Guardian and SIRO for Information Governance related issues.

Staff

All staff (including Medirest, Skanska, agency and contractor colleagues) who use and have access to Trust personal information must understand their responsibilities for data protection and confidentiality.

Contractors and agency staff and other third parties' staff are under instructions to report all incidents, their causes and resolving actions to their own line managers. The Trust reserves the right to audit the supplier's contractual responsibilities or to have those audits carried out by a third party.

The Trust will expect an escalation process for problem resolution relating to any breaches of data security by the contractor's employee and/or any agents and/or sub-contractors.

Any data security breaches made by the contractor's employees, agents or sub-contractors will immediately be reported to the Trust's Information Governance Team sfh-tr.information.governance@nhs.net.

Third parties contracting services to the Trust must sign a confidentiality agreement, countersigned by the Information Asset Owner. This ensures that their employees undertake annual data security awareness training, have read and understood our data protection and

confidentiality policy and accept their personal responsibility to maintain confidentiality at all times.

Managers and health professionals who are responsible for any seconded / work experience placement should ensure that all students have read and understood our data protection and confidentiality policy and accept their personal responsibility to always maintain confidentiality.

5.0 APPROVAL

Data Protection and Cyber Security Committee.

6.0 DOCUMENT REQUIREMENTS

There are four key interlinked strands to Information Governance that this policy, supporting policies and the strategy address:

- Openness
- Legal compliance
- Information security
- Quality assurance.

6.1.1 Openness

- Information about the Trust and its services will be made available to the public in line with the Trust's code of openness.
- The Trust maintains policies and procedures to ensure compliance with the "right to know" principles of the Freedom of Information Act 2000 (FOIA).
- The Trust proactively publishes information under the (FOIA) Publication Scheme in accordance with the Information Commissioner's specifications and will regularly review content.
- Patients have ready access to their information relating to their own health care, their options for treatment and their rights as patients to enable them to make informed choices.

6.1.2 Legal Compliance

- The Trust regards all identifiable personal information and sensitive personal information relating to patients as private and will ensure that it is managed in accordance with the law and duty of confidence.
- The Trust regards all identifiable personal information relating to staff as confidential, except where policy on accountability and openness or the law requires otherwise.
- The Trust maintains policies to ensure compliance with the UK General Data Protection Regulation, Human Rights Act 1998, the Common Law Duty of Confidentiality, and the Freedom of Information Act 2000.

- The Trust maintains policies for the controlled and lawful sharing of confidential patient information with other agencies working in partnerships to provide healthcare services (e.g., [Health and Social Care Act](#), [Crime and Disorder Act](#), [Protection of Children Act](#)).

[Code of Practice on Confidential Information](#)⁴:

“Care must be taken, particularly with confidential clinical information, to ensure that the means of transferring from one location to another are secure as they can be”.

The Caldicott Guardian [Manual](#)⁵ – the Caldicott Guardian should oversee all arrangements, protocols and procedures where confidential patient information may be shared with external bodies both within, and outside, the NHS. This includes flows of information to and from partner agencies, sharing through the NHS Care Records Service (NHS CRS) and related IT Systems, disclosure to research interests and disclosure to the police.

6.1.3 Information Security

- The Trust has appointed a SIRO and established an information risk management structure with IAOs accountable for the management of identified and registered information assets.
- The Trust maintains policies for the effective and secure management of its information assets and resources.
- The Trust promotes effective confidentiality and security practice to its staff through policies, procedures, and training.
- The Trust encourages data security incident reporting, you can find guidance for this within the [Incident Policy](#)⁶ You will also find a detailed guide on how to report an incident using the Trust [Datix System](#) on the Trust Intranet⁷ Through Datix the Trust will monitor and investigate all reported instances of actual or potential breaches of confidentiality and information security.
- **[Information Security Management: NHS Code of Practice](#)**⁸ – all individuals who work within, or under contract to, an NHS organisation have a general responsibility for the security of information that they create or use in the performance of their duties.
- **[UK General Data Protection Regulation \(Principle f\)](#)**⁹: You must ensure that you have appropriate security measures in place to protect the personal data you hold. This is the ‘integrity and confidentiality’ principle of the GDPR – also known as the security principle.

⁴ <https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/code-of-practice-on-confidential-information>

⁵ https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/581213/cgmanual.pdf

⁶ <https://www.sfh-tr.nhs.uk/media/g24emmw4/incident-reporting-policy.pdf>

⁷ <https://sfhnet.nnotts.nhs.uk/content/showContent.aspx?contentId=45809> (Internal website)

⁸ <https://www.gov.uk/government/publications/information-security-management-nhs-code-of-practice>

⁹ <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/integrity-and-confidentiality-security/>

6.1.4 Quality Assurance

The Trust is committed to demonstrating compliance with data security standards through achievement of 'standards met' or 'standards exceeded' of the NHS Digital data security and protection Toolkit and ensuring improvement plans are in place if necessary.

- All staff are personally responsible for the accuracy and quality of information that they hold, obtain, record, use, and share.
- Managers are expected to take ownership of and seek to improve the quality of information within their services.
- Data standards will be set through clear and consistent definitions of data items, in accordance with National Standards.

The Trust promotes the importance of valuable information quality and effective records management through policies, procedures, user manuals, and training. [NHS Information Governance](#) – Guidance on Legal and Professional Obligations¹⁰ – this document lists the relevant legal and professional obligations that limit, prohibit or set conditions in respect of the management, use and disclosure of information and, similarly, a range of statutes that permit or require information to be used or disclosed.

An information asset owner framework will be implemented to ensure ownership of and accountability for the Trust's information assets and the mitigation of associated risks.

Do not...

- Allow personal information to be misused – report incidents.
- Sit on requests for information from the public – Under Freedom of Information Act the Trust has a legal obligation to respond within twenty working days.
- Ignore incorrect/ inaccurate records.
- Keep records beyond retention periods.

¹⁰

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/200702/NHS_Information_Governance_Guidance_on_Legal_and_Professional_Obligations.pdf

7.0 MONITORING COMPLIANCE AND EFFECTIVENESS

Minimum Requirement to be Monitored	Responsible Individual	Process for Monitoring e.g. Audit	Frequency of Monitoring	Responsible Individual or Committee/ Group for Review of Results
(WHAT – element of compliance or effectiveness within the document will be monitored)	(WHO – is going to monitor this element)	(HOW – will this element be monitored (method used))	(WHEN – will this element be monitored (frequency/ how often))	(WHERE – Which individual/ committee or group will this be reported to, in what format (e.g. verbal, formal report etc) and by who)
Legislative Changes	Head of Data Security and Privacy & DPO	Routine monitoring and implementation of legislative changes	Monthly	IG Working Group and Data Protection and Cyber Security Committee

8.0 TRAINING AND IMPLEMENTATION

Training

Annual data security awareness level 1 (formally known as Information Governance) training is mandatory for all new starters as part of the induction process. In addition, all existing staff must undertake data security awareness level 1 training on an annual basis. Staff can undertake this either [face-to-face](#)¹¹ or online. Provision is available online (or face to face for staff who do not have routine access to personal data) and includes Data Protection and confidentiality issues.

Data security awareness level 1 session meets the statutory and mandatory training requirements and learning outcomes for Information Governance in the UK Core Skills Training Framework (UK CSTF) as updated in May 2018¹² to include General Data Protection Regulations (GDPR).

Our Senior Information Risk Owner, Information Asset Owners and Information Asset Administrators must attend regular information risk awareness training which is available from the [Information Governance team](#).

Implementation

A copy of this policy and all related policies and procedures are provided to all staff and patients on the Trust's [website](#).¹³

9.0 IMPACT ASSESSMENTS

This document has been subject to an Equality Impact Assessment, see completed form at Appendix 1.

This document is not subject to an Environmental Impact Assessment.

10.0 EVIDENCE BASE (Relevant Legislation/ National Guidance) AND RELATED SFHFT DOCUMENTS

Evidence Base:

- Refer to list in Appendix 2.

Related SFHFT Documents:

- [Information Security Policy](#)

¹¹ <https://sfhcoursebooking.nnotts.nhs.uk/fulldetails.aspx?recid=195>(internal web link)

¹² <https://www.skillsforhealth.org.uk/wp-content/uploads/2021/07/CSTF-Eng-Subject-Guide-v1.1.pdf>

¹³ <https://www.sfh-tr.nhs.uk/about-us/regulatory-information/non-clinical-policies/>

- [Data Protection, Confidentiality and Disclosure Policy](#), and [Procedure](#)
- [Health Records Management Policy](#)
- [Retention and Destruction Policy](#) and [Procedure](#)
- [Corporate Records Policy](#)
- [Freedom of Information Act Policy](#)

11.0 KEYWORDS

Personal confidential data, confidential information, data, information, availability, integrity, confidentiality.

12.0 APPENDICES

Refer to list in contents table.

APPENDIX 1 - EQUALITY IMPACT ASSESSMENT FORM (EQIA)

Name of service/policy/procedure being reviewed: Information Governance Policy			
New or existing service/policy/procedure: Existing			
Date of Assessment: 25th July 2023			
For the service/policy/procedure and its implementation answer the questions a – c below against each characteristic (if relevant consider breaking the policy or implementation down into areas)			
Protected Characteristic	a) Using data and supporting information, what issues, needs or barriers could the protected characteristic groups' experience? For example, are there any known health inequality or access issues to consider?	b) What is already in place in the policy or its implementation to address any inequalities or barriers to access including under representation at clinics, screening?	c) Please state any barriers that still need to be addressed and any proposed actions to eliminate inequality
The area of policy or its implementation being assessed:			
Race and Ethnicity	None	Not applicable	None
Gender	None	Not applicable	None
Age	None	Not applicable	None
Religion	None	Not applicable	None
Disability	Visual accessibility of this policy	Already in Arial font size 12. Use of technology by end user. This policy can be made available in alternative formats, such as easy read or large print, and may be available in alternative languages, upon request	None
Sexuality	None	Not applicable	None
Pregnancy and Maternity	None	Not applicable	None

Gender Reassignment	None	Not applicable	None
Marriage and Civil Partnership	None	Not applicable	None
Socio-Economic Factors (i.e. living in a poorer neighbourhood / social deprivation)	None	Not applicable	None
What consultation with protected characteristic groups including patient groups have you carried out? <ul style="list-style-type: none"> • None 			
What data or information did you use in support of this EqIA? <ul style="list-style-type: none"> • Trust guidance for completion of the Equality Impact Assessments 			
As far as you are aware are there any Human Rights issues be taken into account such as arising from surveys, questionnaires, comments, concerns, complaints or compliments? <ul style="list-style-type: none"> • None 			
Level of impact Low Level of Impact			
Name of Responsible Person undertaking this assessment: Gina Robinson			
Signature: 			
Date: 18th December 2025			

Appendix 2- List of guidance that has been used to develop this policy.

- **Abortion (Amendment) Regulations 2008**
<http://www.legislation.gov.uk/uksi/2008/735/contents/made>
- **Access to Health Records Act 1990** (where not superseded by the Data Protection Act 1998) <https://www.legislation.gov.uk/ukpga/1990/23/contents>
- **Access to Medical Reports Act 1988** <https://www.legislation.gov.uk/ukpga/1988/28/contents>
- **Article 29 Data Protection Working Party (WP29) Statement 14/EN WP 2186**
<https://ec.europa.eu/newsroom/article29/news-overview.cfm>
- **Audit Commission Act 1998 (repealed)** <http://www.legislation.gov.uk/ukpga/1998/18/contents>
- **Blood Safety and Quality Regulations 2005**
<https://www.legislation.gov.uk/uksi/2005/50/contents>
- **Census (Confidentiality) Act 1991** <https://www.legislation.gov.uk/ukpga/1991/6>
- **Children Act 2004** <http://www.legislation.gov.uk/ukpga/2004/31/contents>
- **Civil Contingencies Act 2004** <https://www.legislation.gov.uk/ukpga/2004/36/contents>
- **Civil Evidence Act 1995** <https://www.legislation.gov.uk/ukpga/1995/38/contents>
- **Computer Misuse Act 1990** <http://www.legislation.gov.uk/ukpga/1990/18/contents>
- **Confidentiality: NHS Code of Practice 2003**
[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/200146/Confidentiality - NHS Code of Practice.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/200146/Confidentiality_-_NHS_Code_of_Practice.pdf)
- **Congenital Disabilities (Civil Liability) Act 1976**
<https://www.legislation.gov.uk/ukpga/1976/28>
- **Consumer Protection Act (CPA) 1987** <https://www.legislation.gov.uk/ukpga/1987/43>
- **Control of Substances Hazardous to Health (COSHH) Regulations 2002**
<https://www.legislation.gov.uk/uksi/2002/2677/regulation/7>
- **Copyright, Designs and Patents Act** <https://www.legislation.gov.uk/ukpga/1988/48/contents>
(as amended by the Copyright (Computer Programs) Regulations 1992
<https://www.legislation.gov.uk/uksi/1992/3233/made>
- **Crime and Disorder Act 1998** <http://www.legislation.gov.uk/ukpga/1998/37/contents>
- **Criminal Appeal Act 1995** <https://www.legislation.gov.uk/ukpga/1995/35/contents>
- **Data Protection Act 2018** <http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>
- **Disclosure of Adoption Information (Post-Commencement Adoptions) Regulations 2005**
<https://www.legislation.gov.uk/uksi/2005/888/contents>
- **Electronic Commerce (EC Directive) Regulations 2002**
<https://www.legislation.gov.uk/uksi/2002/2013/contents>
- **Electronic Communications Act 2000** <https://www.legislation.gov.uk/ukpga/2000/7/contents>
- **Environmental Information Regulations (EIR) 2004**
<https://www.legislation.gov.uk/uksi/2004/3391/contents>
- **Freedom of Information Act 2000** <https://www.legislation.gov.uk/ukpga/2000/36/contents>
- **Gender Recognition Act 2004** <https://www.legislation.gov.uk/ukpga/2004/7/contents>

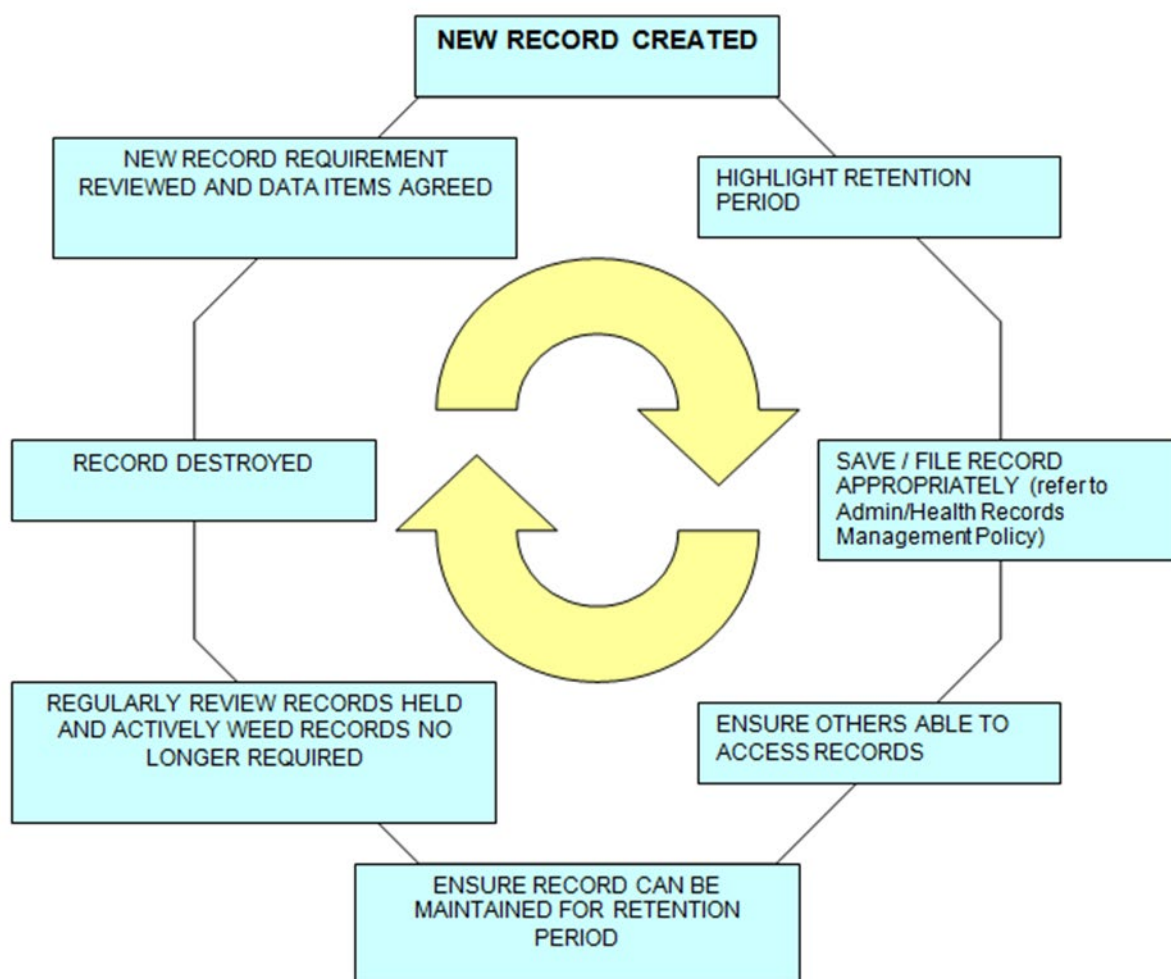
- **General Data Protection Regulation (EU) 2016** <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679>
- **Health and Safety at Work etc. Act 1974** <http://www.legislation.gov.uk/ukpga/1974/37/contents>
- **Health and Social Care (Safety and Quality) Act 2015** <https://www.legislation.gov.uk/ukpga/2015/28/contents>
- **Health and Social Care Act 2008** <https://www.legislation.gov.uk/ukpga/2008/14/contents>
- **Health and Social Care Act 2012** <http://www.legislation.gov.uk/ukpga/2012/7/contents/enacted>
- **Human Fertilisation and Embryology Act 1990** <http://www.legislation.gov.uk/ukpga/1990/37/contents>
- **Human Rights Act 1998** <https://www.legislation.gov.uk/ukpga/1998/42/contents>
- **Information: To share or not to share? The Information Governance Review March 2013** https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf
- **ISO/IEC 27002:2022** (Information Security Standards) <https://www.iso.org/standard/75652.html>
- **ISO/IEC 27001: 2022** <https://www.iso.org/standard/54534.html>
- **Limitation Act 1980** <https://www.legislation.gov.uk/ukpga/1980/58>
- **Medicines for Human Use (Clinical Trials) Amendment Regulations 2006** <https://www.legislation.gov.uk/uksi/2006/1928/contents/made>
- **NHS Act 2006** <https://www.legislation.gov.uk/ukpga/2006/41/contents>
- **NHS Care Record Guarantee** <https://webarchive.nationalarchives.gov.uk/ukgwa/20131104121019/http://www.nigb.nhs.uk/public/nhscrg.pdf>
- **NHS Constitution for England** <https://www.gov.uk/government/publications/the-nhs-constitution-for-england>
- **NHS Digital Information Governance** <http://systems.digital.nhs.uk/infogov>
- **Police and Criminal Evidence (PACE) Act 1984** <https://www.legislation.gov.uk/ukpga/1984/60/contents>
- **Prevention of Terrorism Act 2005** <https://www.legislation.gov.uk/ukpga/2005/2/section/16>
- **Privacy and Electronic Communications (EC Directive) Regulations 2003** <https://www.legislation.gov.uk/uksi/2003/2426/contents>
- **Public Health (Control of Diseases) Act 1984** <https://www.legislation.gov.uk/ukpga/1984/22>
and the **Public Health (Infectious Diseases) Regulations 1988** <https://www.legislation.gov.uk/uksi/1988/1546/made>
- **Public Interest Disclosure Act 1998** <https://www.legislation.gov.uk/ukpga/1998/23/contents>
- **Public Records Act 1958** <https://www.legislation.gov.uk/ukpga/Eliz2/6-7/51>
- **Radioactive Substances Act 1993** <https://www.legislation.gov.uk/ukpga/1993/12/contents>
- **Records Management Code of Practice 2021** <https://www.nhsx.nhs.uk/information-governance/guidance/records-management-code/>
- **Regulation of Investigatory Powers Act 2000** <http://www.legislation.gov.uk/ukpga/2000/23/contents>

- **Re-use of Public Sector Information Regulations 2005**
<https://www.legislation.gov.uk/uksi/2005/1515/contents>
<http://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/>
- **Road Traffic Acts 1991** <https://www.legislation.gov.uk/ukpga/1991/40/contents>
- **Sexual Offences (Amendment) Act 1976, sub-section 4(1), as amended by the Criminal Justice Act 1988** <https://www.legislation.gov.uk/ukpga/1976/82>
- **Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000** <https://www.legislation.gov.uk/uksi/2000/2699/contents/made>
- **UK General Data Protection Regulation**
<https://www.legislation.gov.uk/ukpga/2018/12/contents>
- **WP29 Guidelines on Data Protection Officer 16/EN WP 2437**
https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A
- **WP29 Opinion on Purpose limitation 13/EN WP 2038**
<https://ec.europa.eu/newsroom/article29/news-overview.cfm>

Appendix 3 - Information Lifecycle Management Strategy

Within the Trust, all staff creating any type of record (paper or electronic) are required to liaise with their division records manager to ensure the appropriate Records Management Policy is implemented. For every item of information created, there will be a time period (retention period) for which it is required and must be accessible. These are outlined in the Records Management Code of Practice 2021¹⁴ and [Retention and Destruction Policy](https://www.sfh-tr.nhs.uk/media/2jcn1rij/retention-and-destruction-policy.pdf)¹⁵. Once information has reached the end of its period of retention, the records must be reviewed and if no longer appropriate to retain the record it must be securely destroyed in line with Trust policy. Further advice is available from the Information Governance team sfh-tr.information.governance@nhs.net.

Figure 1 – Records Management Life Cycle



¹⁴ <https://www.sfh-tr.nhs.uk/media/lmsnfm4c/records-management-code-of-practice.pdf>

¹⁵ <https://www.sfh-tr.nhs.uk/media/2jcn1rij/retention-and-destruction-policy.pdf>