CORPORATE RECORDS POLICY

POLICY

Reference	IG001		
Approving Body	Information Governance Committee		
Date Approved	7th February 2025		
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**	**N/A**
	x		
Issue Date	*Enter the date the document is effective from*		
Version	5		
Summary of Changes from Previous Version	Minor changes to external references and terminology of roles		
Supersedes	4		
Document Category	Information Governance		
Consultation Undertaken	Information Governance Working Group		
Date of Completion of Equality Impact Assessment	14th January 2025		
Date of Environmental Impact Assessment (if applicable)	Not applicable		
Legal and/or Accreditation Implications	Failure to comply with: • Public Records Act 1958 • Freedom of Information Act 2000 • UK GDPR and Data Protection Act 2018 • Health and Social Care Act 2008		
Target Audience	All staff		
Review Date	31st January 2027		
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		

Associated Documents/ Information	Date Associated Documents/ Information was reviewed
1. Records Management Code of Practice Updated August 2023	August 2023
2. Retention and Destruction Policy	January 2025
3. Retention and Destruction Procedure	April 2023
Template control	April 2024

CONTENTS

APPENDICIES

1.0 INTRODUCTION

Sherwood Forest Hospitals NHS Foundation Trust (the Trust) is dependent on its records to operate efficiently and account for its actions. This policy defines a structure for the Trust, which supports the Records Management Code of Practice for Health and Social Care 2021 to ensure adequate corporate records are maintained and that they are managed and controlled effectively and at best value, in keeping with legal, operational and information needs.

The Trust's records are our corporate memory, providing evidence of actions and decisions and representing a vital asset to support our daily functions and operations. They support policy formation and managerial decision-making, protect the interests of the Trust and the rights of patients, staff and members of the public who have dealings with the Trust.

They support consistency, continuity, efficiency, and productivity and help us deliver our services in consistent and equitable ways. Records management, through the proper control of the content, storage, and volume of records, reduces vulnerability to legal challenge or financial loss and promotes best value in terms of human and space resources through greater co-ordination of information and storage systems. Information is of greatest value when it is accurate, up to date and accessible when needed.

An effective corporate records management service ensures that information is properly managed and available to those with a legitimate need.

All NHS records are classified as 'public records' under the Public Records Act 1958. Schedules 3(1) – (2) state that they must be kept in accordance with statutory and NHS guidelines including:

'This policy is issued and maintained by the Director of Corporate Affairs (the sponsor) on behalf of the Trust, at the issue defined on the front sheet, which supersedes and replaces all previous versions.'

Employees are responsible for any records that they create or use in the course of their duties. This includes records controlled by NHS organisations under contractual or other joint arrangements, or as inherited legacy records of defunct NHS organisations. The Act applies regardless of the format of the records.

The Freedom of Information Act (FOIA) governs access to and management of non-personal public records. The FOIA was designed to create transparency in government and allow any citizen to know about the provision of public services through the right to submit a request for information. This right is only as good as the ability of those organisations to supply information through good records management programmes. Records managers should adhere to the code of practice on record keeping[1] issued by the Secretary of State for Culture, Media and Sport, under section 46 of the FOIA. The section 46 Code of Practice is used as a statutory statement of good practice by the regulator and the courts.

Section 47 of FOIA places a duty on the Information Commissioner to promote the following of good practice by public authorities and the observance by them, of FOIA and codes of practice

[1] https://www.gov.uk/government/publications/code-of-practice-on-the-management-of-records-issued-under-section-46-the-freedom-of-information-act-2000

The UK GDPR is the principal legislation governing how records, information and personal data are managed. It sets in law how personal and special categories of information may be processed. The Data Protection Act 2018 principles are also relevant to the management of records. Under the UK GDPR, organisations may be required to undertake Data Protection Impact Assessments (DPIA) as set out in Section 3 of this Records Management Code.

The UK GDPR also introduces a principle of accountability. The Information Commissioner's Office (ICO) Accountability Framework[2] can support organisations with their obligations. Good records management will help organisations to demonstrate compliance with this principle.

Regulation 17 under the Health and Social Care Act 2008 requires that health and care providers must securely maintain accurate, complete, and detailed records for patients or service users, employment of staff and overall management. The CQC are responsible for regulating this and have issued guidance on regulation 17. The CQC may have regard to the Code when assessing providers' compliance with this regulation

Other legislation requires information to be held as proof of an activity against the eventuality of a claim. Examples of legislation include the Limitation Act 1980 or the Consumer Protection Act 1987. The Limitation Act sets out the length of time you can bring a legal case after an event.

2.0 POLICY STATEMENT

The Trust acknowledges the importance of records and is committed to create, keep, maintain, and dispose of records, including digital records, in line with legal, operational and information leads.

The Trust is committed to ensuring that none of its policies, procedures and guidelines discriminate against individuals directly or indirectly based on gender, colour, race, nationality, ethnic or national origins, age, sexual orientation, marital status, disability, religion, beliefs, political affiliation, trade union membership, and social and employment status.

3.0 DEFINITIONS/ ABBREVIATIONS

In this policy:

'**Corporate records**': Information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business This definition does not relate to health records. Administrative records include both paper and digital records.

'**Governance manual**': Means the manual of governance documents, including the standing orders, standing financial instructions and scheme of delegation.

'**SIRO**': Means 'Senior Information Risk Owner'; responsible for leading and implementing the information risk management process and providing Board assurance.

[2] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/a-guide-to-data-security/

'**IAO**': Means 'Information Asset Owner'; responsible for understanding and assessing the information they 'own' and providing the SIRO with assurance in relation to the security of that asset. They will also coordinate compliance with this policy.

'**IAA**': Means 'Information Asset Administrator'; responsible for providing support to their IAOs in ensuring that IG policies are followed, and that information risks and incidents are documented and escalated accordingly.

'**Staff**': Means all employees of the Trust including Medirest, Skanska, agency and contractor colleagues.

The '**PRA**': Means the Public Records Act 1958

The '**DPA**': Means the Data Protection Act 2018

The '**policy**': Means the Corporate Records Policy

The '**Trust**': Means Sherwood Forest Hospitals NHS Foundation Trust

'**IG**': Means Information Governance.

4.0 ROLES AND RESPONSIBILITIES

Statutory Responsibility:
The Secretary of State for Health and all NHS organisations have a duty under the Public Records Act 1958 (PRA) to make arrangements for the safe keeping and eventual disposal of all types of their records. This is carried out under the overall guidance and supervision of the Keeper of Public records who is answerable to parliament. Chief Executives and Senior Managers of all NHS organisations are personally accountable for records management within their organisations.

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, Caldicott Guardian, Data Protection Officer, and members of the Information Governance Committee. Trust Board has responsibility, in compliance with the Trust's Governance manual, to ensure and gain assurance that the Trust has in place robust arrangements for the management of records and that such arrangements are complied with.

Senior Information Risk Owner (SIRO)
The Director of Corporate Affairs is responsible to the Chief Executive for Information Governance and is the designated Senior Information Risk Owner, 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 Senior Information Risk Owner also reports annually to the Trust Board on Information Governance performance.

Caldicott Guardian
The Caldicott Guardian (a role currently undertaken by 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
As a public authority we have appointed a Data Protection Officer who is also the Head of Data Security and Privacy. The Data Protection Officer reports to the Senior Information Risk Owner and works with the Caldicott Guardian. The Data Protection Officer is tasked with monitoring compliance with Data Protection legislation, our data protection policies, awareness raising, training, and audits. The Data Protection Officer acts as a contact point for the Information Commissioner's Office. When performing their tasks, the Data Protection Officer 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 can 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. Record Management responsibilities will be written into all accountable individuals' job descriptions.

Information Asset Administrators
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, they seek the advice of the Trust's Data Protection Officer who also monitors the process. Information Asset Administrators will liaise with the Information Governance Team on the management of records in that division/speciality/department. The Information Governance Team will provide support and guidance to nominated departmental representatives.

5.0 APPROVAL

Information Governance Committee
The Information Governance Committee is responsible for ensuring that this policy is effectively implemented, including any supporting guidance and training deemed necessary to support the implementation, and for monitoring and providing Board assurance in this respect.

6.0 DOCUMENT REQUIREMENTS

For this policy, a document becomes a record when it has been finalised and becomes a part of the corporate information*.

This policy relates to records held in any format, both paper and digital including e-mails. It does not relate to health records or patient case notes, please refer to the Health Records Management Policy.

The ISO standard ISO 15489-1:2016[3] defines a record as: 'Information created, received, and maintained as evidence and as an asset by an organisation or person, in pursuance of legal obligations or in the transaction of business.'

*Corporate information refers to information generated by the Trust, that is not confidential patient information. Corporate information describes the records generated by an organisation's business activities and therefore will include records from the following areas of the Trust, but are not restricted to:

- Clinical Governance
- Commercial and communications activities
- Commissioning and contracts
- Complaints, Concerns and Compliments
- Estates
- Facilities
- Finance
- Health care quality and clinical audit
- Human Resources, organisational development, and training
- ICT
- Information Governance
- Performance management
- Procurement
- Strategic Planning and Commercial Development
- Trust Board Business

This policy relates to the management of all administrative records of the Trust, as detailed above, including but not limited to:

- Accounting records and budgetary information
- Board, committee, sub-committee, and all other meeting minutes
- Contracts
- Databases
- Diaries
- Standing Financial Instructions
- Invoices
- Litigation dossiers, including complaints, claims, and inquest files
- Minutes and agendas
- Payroll/PAYE records
- Policies and procedures
- Policy and procedure manuals
- Public Consultations
- Reports (e.g. annual, accounting, Board)

[3] https://www.iso.org/standard/62542.html

- Spread sheets
- Strategies and action plans
- Staff records
- VAT records

All records created during the business of the Trust are public records under the terms of the Public Records Act.

Good records management should be seen as a benefit, not a burden.

This policy does not address the retention and ultimate destruction (or permanent preservation) of records. These matters are covered by two separate complementary policies; Retention and Destruction Policy and Records Management Code of Practice for Health and Social Care 2021, updated August 2023, both available on the website.

Record keeping systems must have a means of physically or digitally organising records. Further advice is available in the Retention and Destruction Policy and Procedure available on the website.

Wherever possible, the Trust intends to move to digital records. The original paper record guarantees the authenticity of the record. However, it can make it hard to audit access to the record, depending on where this is stored, because paper records do not have automatic audit logs.

Where possible, paper records management processes should be as environmentally friendly as possible. This will help contribute towards the NHS target to reduce its carbon footprint and environmental impact.

Digital records offer many advantages over paper records. They can be accessed simultaneously by multiple users, take up less physical storage space and enable activities to be carried out more effectively, for example, using search functions and digital tools. Digital information must be stored in such a way that, throughout its lifecycle, it can be recovered in an accessible format in addition to providing information about those who have accessed the record.

Digital information presents a unique set of issues which must be considered and overcome to ensure that records remain:

- authentic
- reliable
- retain their integrity
- retain usability.

Records for permanent preservation

The Public Records Act 1958 requires organisations to select records for permanent preservation. Selection for transfer under this Act is separate to the operational review of records to support current service provision. It is designed to ensure the permanent preservation of a small core (typically 2-5%) of key records, which will:

- enable the public to understand the working of the organisation and its impact on the population it serves
- preserve information and evidence likely to have long-term research or archival value.

Records for preservation must be selected in accordance with the guidance issued in the Records Management Code of Practice. Any supplementary guidance issued by The National Archives and Nottinghamshire Archives should always be consulted in conjunction with the Information Governance team, in advance of any possible accession. This is to ensure it is appropriate to transfer the records selected.

NHS records when the minimum retention period is reached will accession their records to the Nottinghamshire Archives, as appointed by the Secretary of State for Culture, Media, and Sport. Selection may take place at any time in advance of transfer. However, the selection and transfer must take place at or before records are 20 years old. Records may be selected as a class (for example, all board minutes) or at lower levels down to individual files or items.

Records can be categorised as follows:

- transfer to Nottinghamshire Archives - this class of records should normally transfer in its entirety to the PoD – trivial or duplicate items can be removed prior to transfer
- consider transfer to Nottinghamshire Archives - all, some or none of this class may be selected (as agreed with the PoD)
- no Nottinghamshire Archives interest.

Transfers of records to the Nottinghamshire Archives

Records selected for permanent preservation should be transferred to the Nottinghamshire Archives. Current contact details of Nottinghamshire Archives archives@nottscc.gov.uk, 0115 958 1634. The organisations which should transfer to them can be found on The National Archives website[4].

Public and Statutory Inquiries

There are two statutory public inquiries which have requested that large parts of the health and social care sector do not destroy any records that are, or may fall into the remit of the Inquiry:

1. The Infected Blood Inquiry - Investigates the circumstances in which NHS patients were given infected blood and blood products. Further information about the records required can be found on the Inquiry website[5].

2. COVID-19 Inquiry – Investigates issues related to the COVID-19 pandemic. Further information is available here: UK COVID-19 Inquiry: terms of reference - GOV.UK (www.gov.uk)[6]. SFHFT have created records specifically in response to a pandemic, these should not be destroyed when they have reached their minimum retention period, unless the public Inquiry has ended, or the Inquiry has provided guidance on what type of records it will

[4] https://www.nationalarchives.gov.uk/information-management/manage-information/places-of-deposit/
[5] https://www.infectedbloodinquiry.org.uk/
[6] https://www.gov.uk/government/publications/uk-covid-19-inquiry-terms-of-reference/uk-covid-19-inquiry-terms-of-reference#:~:text=The%20Inquiry%20will%20examine%2C%20consider,up%20date%2C%2028%20June%202022
.

be interested in. These specific records may have historical value, so discussions must take place with Information Governance.

Retention schedule

The retention periods listed in the retention schedule must always be considered the minimum period.

You can search the retention schedule here: Records Management Code of Practice 2021 - NHS Transformation Directorate (england.nhs.uk)

7.0 MONITORING COMPLIANCE AND EFFECTIVENESS

Minimum Requirement to be Monitored (WHAT – element of compliance or effectiveness within the document will be monitored)	Responsible Individual (WHO – is going to monitor this element)	Process for Monitoring e.g. Audit (HOW – will this element be monitored (method used))	Frequency of Monitoring (WHEN – will this element be monitored (frequency/ how often))	Responsible Individual or Committee/ Group for Review of Results (WHERE – Which individual/ committee or group will this be reported to, in what format (e.g verbal, formal report etc) and by who)
Review of inventory of corporate records	Head of Data Security and Privacy	Review	Annually	IG Team
Adherence to Corporate Records Policy to DPA, FOI and other IG areas	Head of Data Security and Privacy	Monitor	Annually	IG Team
Datix incidents relating to Corporate records	Head of Data Security and Privacy	Audit	Monthly	IG Team

8.0 TRAINING AND IMPLEMENTATION

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 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 2018 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.[7]

9.0 IMPACT ASSESSMENTS

- This document has been subject to an Equality Impact Assessment, see completed form at Appendix 1
- This document has been subject to an Environmental Impact Assessment, see completed form at Appendix 2.

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

Evidence Base:
- Freedom of Information Act 2000
- Freedom of Information Act Section 45 Code of Practice[8]
- Freedom of Information Act Section 46 Code of Practice[9]
- Health and Social Care Act 2008
- Limitation Act 1980
- Public Records Act 1958
- Records Management Code of Practice for Health and Social Care 2021, updated August 2023
- Re-use of Public Sector Information Regulations 2015
- UK GDPR and Data Protection Act 2018

[7] https://www.sfh-tr.nhs.uk/about-us/policies-and-procedures/non-clinical-policies-procedures/information-governance/
[8] https://ico.org.uk/for-organisations/guidance-index/freedom-of-information-and-environmental-information-regulations/section-45-code-of-practice-request-handling-1/
[9] https://ico.org.uk/media/for-organisations/documents/1624142/section-46-code-of-practice-records-management-foia-and-eir.pdf

Related SFHFT Documents:

- Data Protection, Confidentiality and Disclosure Policy
- Data Protection, Confidentiality and Disclosure Procedure
- E-mail and Internet Policy
- Freedom of Information Act Policy
- Health Records Management Policy
- IAO Framework
- Information Governance Policy
- Information Security Policy
- Retention and Destruction Policy

11.0 KEYWORDS

Records, management.

12.0 APPENDICES

List in contents table.

APPENDIX 1 - EQUALITY IMPACT ASSESSMENT FORM (EQIA)

Name of service/policy/procedure being reviewed: Corporate Records Policy			
New or existing service/policy/procedure: Existing			
Date of Assessment: 14th January 2025			
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 / Belief	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? • None			
What data or information did you use in support of this EqIA? • Trust guidance for completion of 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? • No			
Level of impact Low Level of Impact			
Name of Responsible Person undertaking this assessment: Gina Robinson			
Signature:			
Date: 14th January 2025			