RETENTION AND DESTRUCTION POLICY

POLICY

Reference	ISP-10		
Approving Body	Information Governance Committee		
Date Approved	18th March 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	18th March 2025		
Version	10		
Summary of Changes from Previous Version	Updated with local arrangements for the destruction of health records and occupational health records		
Supersedes	9		
Document Category	Information Governance		
Consultation Undertaken	Information Governance Working Group Information Governance Committee		
Date of Completion of Equality Impact Assessment	23rd January 2025		
Date of Environmental Impact Assessment (if applicable)	23rd January 2025		
Legal and/or Accreditation Implications	Legal: • Data Protection Act 2018 • UK General Data Protection Regulation • Common law duty of confidentiality • Freedom of Information Act 2000 • Public Records Act 1958 • The key principles outlined within the policy in relation to disposal of records after scanning arise from the Civil Evidence Act 1995 and are supported in respect of criminal prosecutions by the Policy and Criminal Evidence Act 1984. Accreditation: • Care Quality Commission • NHS England Data Security and Protection Toolkit • MHRA		
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

Associated Documents/ Information	**Date Associated Documents/ Information was reviewed**
• Suite of Information Governance Policies and Procedures	13th January 2023
• Quality Assurance Guidance - Legal Admissibility of Scanned Digital Health Records	
• Records Management Code of Practice Updated August 2023	August 2023
• Retention and Destruction Procedure	April 2023
Template control	April 2024

CONTENTS

APPENDICIES

1.0 INTRODUCTION

Sherwood Forest Hospitals NHS Foundation Trust (the Trust) adheres to the retention and disposal of all corporate and clinical records to ensure compliance with legal obligations. In addition to this, the policy allows the Trust to effectively manage storage space and the cost of preservation for paper and digital records.

This policy relates to all records, including 'health records'. The term 'health record' applies to a record relating to the physical or mental health of a given patient/client who can be identified from that information and has been recorded by or on behalf of a health professional in connection with the care of that patient/client.

All NHS records are public records under the terms of the Public Records Act 1958. Schedules 3(1) – (2) 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.'

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.

Retention and disposal scheduling of records is an important aspect of governance of patient information and resources. Not all health records can or should be retained indefinitely. The benefits of effective records management are:

- Protecting business critical records and improving business resilience
- Ensuring information can be found and retrieved quickly and efficiently
- Complying with legal and regulatory requirements
- Reducing risk for litigation, audit and investigations
- Minimising storage requirements and reducing costs.

This policy sets out the Trust's approach to retention, disposal and lifecycle management of health records and data and also the Trust's commitment to only retain health records for as long as required for patient healthcare or other specific NHS purpose, thereby complying with the following legislative requirements and guidance:

- Data Protection Act 2018 and the UK General Data Protection Regulation principle Article 5 (e) in that personal data must not be kept longer than is necessary

[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

- Records Management Code of Practice for Health and Social Care 2021 (RMCoP)
- NHS England Data Security and Protection Toolkit
- Care Quality Commission
- Public Records Act 1958.

Scope

This policy applies to all records, including confidential patient information ie health records.

The ISO standard ISO 15489-1:2016[2] 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.'
It includes information in all media formats including paper and digital records held in IT systems maintained by ICT Services or by clinical or ancillary departments. This list is not exhaustive.

This policy forms part of and should be read in conjunction with a framework of Information Governance policies and procedures which are available on our website[3].

The way in which information is recorded and maintained within an organisation is critical to effective business function. The way in which records are controlled is essential for the continuity of efficient and effective working practices throughout the Trust. Without this consideration, records quickly become disorganised and useless.

The destruction of records is an irreversible act which may have serious consequences. Conversely, data protection legislation makes it unlawful to retain health records for longer than it is needed.

This policy ensures that appropriate controls are in place so that records are retained lawfully, irreversible errors are prevented and that governance is appropriately directed through policy procedures and audit. This policy also provides the Trust with the legal basis for retaining or disposing of patient records.

The Trust's foremost intentions are:

- to comply with data protection legislation and other legal, statutory and regulatory requirements;
- to demonstrate that records are only retained for as long as needed for patient care or other legitimate NHS activity;

[2] https://www.iso.org/standard/62542.html
[3] https://www.sfh-tr.nhs.uk/about-us/policies-and-procedures/non-clinical-policies-procedures/information-governance/

- to demonstrate that disposal of patient information is carried out according to an agreed policy;
- to ensure disposal decisions and execution are taken with proper authority and are fully auditable;
- to avoid the costs and potential liabilities of retaining personal data that the Trust no longer needs;
- to minimise the administrative and storage overhead of expired data.

Do's and Don'ts

☑ DO – consider how records will be managed over their lifetime when procuring/ developing systems
☑ DO make sure that any Divisional/Departmental information assets which contain patient identifiable health record information are registered on the Trust's Information Asset Register (IAR) and that they fully comply with this policy
☑ DO use and comply with the retention schedules within the Records Management Code of Practice 2021 and look up minimum retention periods. 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)[4]
☑ DO build in annual appraisal and disposal into records management procedures for all records collections/information asset holdings
☑ DO ensure the Information Asset Register (IAR) is used as a Master Disposal Register to record all records and information assets disposed of.

☒ DON'T work under a misconception that patient identifiable records can be held indefinitely simply because they are held digitally
☒ DON'T create or retain patient identifiable records that are not registered on the Information Asset Register.

Local business requirement/instructions must be considered before activating retention periods in this schedule. Decisions should also be considered in the light of the need to preserve records, whose use cannot be anticipated fully at the present time, but which may be of value to future generations.

- Recommended minimum retention periods should be calculated from the end of the calendar or accounting year following the last entry on the document.
- The selection of files for permanent preservation is partly informed by precedent and partly by historical content.
- The provision of the Data Protection Act must be complied with.

[4] https://transform.england.nhs.uk/information-governance/guidance/records-management-code/records-management-code-of-practice/#appendix-ii-retention-schedule

- Non active records should be transferred no later than 30 years from the creation of the record as required by the Public Records Act 1958.
- A record of the destruction of the records, showing their reference, description and date of destruction will be maintained and preserved so that the Trust can accurately identify which of those records have been destroyed and are no longer available.

2.0 POLICY STATEMENT

Data Protection Legislation

By adopting this policy the Trust aims to comply with data protection legislation in that 'personal data shall be kept in a form which permits identification of data subjects no longer than is necessary for the purposes for which the personal data is processed'. The ICO guidance Deleting personal data[5] sets out that if information is deleted from a live environment and cannot be readily accessed, then this will suffice to remove information for the purposes of UK GDPR. Their advice is to only procure systems that will allow permanent deletion of records to allow compliance with the law.

The Trust Board recognises the importance of efficient and effective records management and is committed to create, keep, maintain and dispose of records, including digital records, commensurate with legal, operational and information needs.

The Records Management Code of Practice 2021 Retention Schedules

The Trust aims to comply with the Records Management Code of Practice 2021 (RMCoP) published by NHS England. This sets out good practice requirements for the management of NHS records, including retention schedules and compliance with the Public Records Act and other relevant legislation. Retention schedules reflect minimum clinical need/requirement or legal value.

Wherever practicable the Trust will not retain health records and information beyond the minimum retention periods in Records Management Code of Practice 2021 schedules unless extended or permanent preservation for a specific category of record has been agreed via the Information Governance Committee, recorded in the Appendix 4 of this policy and within the provisions of the Appraisal Process within this policy.

Where it is not feasible to appraise individual records collections/ information based on clinical diagnosis the Trust will identify and archive non-current records advised by audit data on when they were last clinically accessed.

Disposal of documents/records after scanning

[5] https://ico.org.uk/media/for-%20organisations/documents/1475/deleting_personal_data.pdf

To confirm appropriate legal admissibility of digital records the Trust must be able to demonstrate that scanned documents and processes are compliant with the legally recognised standard BS10008 which requires documents to be validated as authentic, in that they have been scanned to specific standards, are unaltered since the time of digital storage and that they are a reliable and true representation of the original paper record.

Via a combination of defined acceptance requirements and audit processes the Trust will be able to provide evidence that BS10008 standards are met, that records are legally admissible and that disposal of source records after the scanning process represents a minimal and acceptable risk. Section 4.5.1 of the Retention and Destruction Procedure deals specifically with disposal of paper (source) health record documents after scanning.

3.0 DEFINITIONS/ ABBREVIATIONS

Appraisal - the process of deciding what to do with records once their business need has ceased and the minimum retention period has been reached. This can also be known as the disposition of records. The National Archives has produced guidance on appraisal[6].

Beyond use - Within the guidance document Deleting Personal Data (Information Commissioner's Office). Once recorded information is put 'beyond use' the Trust:

• Is not able, or will not attempt, to use the personal data to inform any decision in respect of any individual or in a manner that affects the individual in any way;
• will not give any other organisation access to the personal data;
• will surround the personal data with appropriate technical and organisational security; and
• commits to permanent deletion of the information if, or when, this becomes possible.

Closure - Removal or erasure of information from paper storage, digital devices and other storage media by marking a record as 'closed'. The information still exists, making data recovery possible. This is helpful if a mistake has been made, however, it does not permanently and securely delete data.

Digital records - are both records created digitally i.e. 'born digital' or digitised by conversion to digital format e.g. by scanning.

Migration - is, for the purposes of this policy, any activity undertaken to move data from one system or platform to another. Migration may occur between major version upgrades of a system, or between applications on different platforms.

[6] https://www.nationalarchives.gov.uk/information-management/manage-information/selection-and-transfer/

Non- current – For the purposes of this policy this constitutes any record which has not been accessed in the last 8 years.

Secure Deletion - Means the process of deliberately, permanently, and irreversibly removing erasing or rendering unreadable information from digital devices and storage media.

CareFlow EPR – Patient Administration System.

Permanent Preservation - Records deemed suitable for permanent preservation as required by the Public Records Acts 1957 and 1958 and which will be offered to a Place of Deposit approved by the Nottinghamshire Archives who may accept or decline.Further information is available in section 6 of the corporate records policy. .

Personal data - 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.

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.

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.

Examples of personal data include:

- a name
- an identification number i.e. NHS number, NI number
- location data
- an online identifier
- one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of personal data - The special categories of personal data are:

a. racial or ethnic origin
b. political opinions
c. religious or philosophical beliefs
d. trade-union membership
e. genetic data
f. biometric data for the purpose of uniquely identifying a natural person
g. data concerning health
h. data concerning a natural person's sex life or sexual orientation.

Glossary

Records	Means all records completed and held in respective of the Trust's business that contain information relating to both healthcare and administration. Records include both paper based and digital records
The PRA	Means the Public Records Act 1958
The Trust	Means Sherwood Forest Hospitals NHS Foundation Trust

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 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 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. Our Data Protection Officer acts as a contact point for the Information Commissioner's Office. When performing their tasks, our 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 our 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 directorate/speciality/department. The Information Governance Team will provide support and guidance to nominated departmental representatives.

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

5.0 APPROVAL

This policy will be approved at the Information Governance Committee.

6.0 DOCUMENT REQUIREMENTS

6.1 Disposal Policy and Schedules

Where technically possible the Trust will ensure that health records of any format when no longer required for patient care/specified Trust purposes are archived to a non-current status

and disposed of, 'closed' or 'put beyond use' in accordance with the disposal schedules within the Records Management Code of Practice 2021.

In the event that prior disposal is not technically possible, no record will be retained beyond the longest retention timescale of 30 years after last contact.

6.2 Retention and Continued Accessibility

Records in any formats required for continued retention will be stored in such a way throughout their lifecycle that information can continue to be accessed and recovered in addition to providing information about those who have accessed the record, as required by the Care Record Guarantee (Information Governance Alliance, 2016).

6.3 Technical Capability

The Trust will procure IT systems which facilitate appropriate records lifecycle management including appraisal, archiving and permanent deletion of recorded information. Assurances of appropriate capability and functionality will form part of the procurement process and the Data Protection Impact Assessment for all new and changed IT systems.

6.4 Appraisal Process

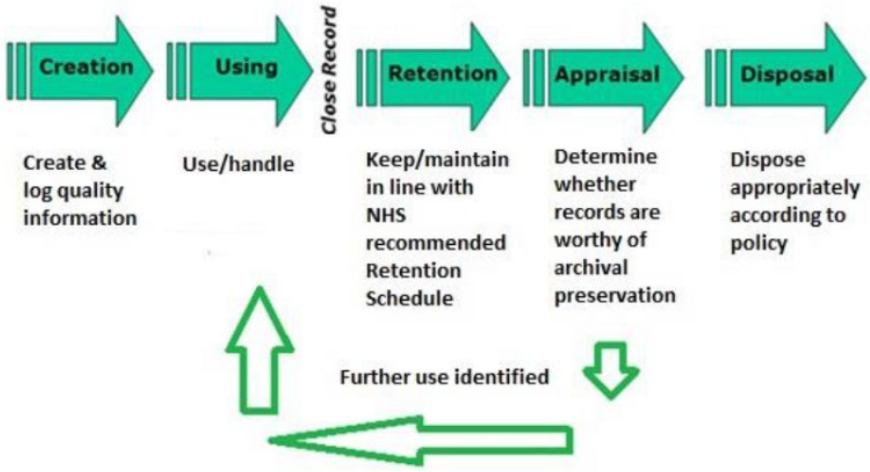
Information Asset Owner's and administrators will be required to provide assurance to the Information Governance Committee that a standard concept of records lifecycle management is applied via an annual appraisal of records. Information assets registered on the Information Asset Register (IAR) which:

- Identifies records that need to be retained for a longer period as they are still in use, or;
- Are worthy/have Trust agreement for extended or archival preservation (see Appendix 4), or;
- Can be put 'closed' from continued access (marked as closed and transferred to secondary storage)
- Can be securely destroyed/deleted or 'put beyond use' if deletion is not technically possible.

If as a result of appraisal, a decision is made to destroy or delete a record, there must be evidence of the decision using appendix 3 of this policy. Authorisation for destruction or deletion is required from the Information Governance Committee.

Where the destruction or deletion process is new, or there is a change in the destruction process (such as a change of provider, or the method used), a DPIA must be completed and signed off by the Information Governance Committee.

Figure 1 - The Records/Information Lifecycle



6.5 Appraisal and Disposal of Health Records held in digital Systems

Although there are legal and economic reasons to dispose of digitally held records in line with the Records Management Code of Practice 2021 retention schedule, there are a number of issues which may currently prevent the Trust and similar NHS organisations from implementing a continuing and rolling programme of digital health records disposal across all systems.

Within an Acute hospital setting health records are held on a complicated variety of linked IT legacy systems. At present there are a number of challenges which prevent a rolling and automated disposal process for digital health records.

These issues are:

- The number of systems involved and a technical inability to map and link disposal to specific patient records held in individual but linked systems;
- Disposal tools/functionality within individual legacy systems is either not present or difficult or ineffectual to use, these systems are gradually being replaced by procurement of new systems which allow permanent deletion;
- Interdependency of systems for data;
- The Records Management Code of Practice 2021 based timescales for retention and disposal of patient records on patient diagnosis and date of last attendance. e.g. oncology records have to be retained for 30 years, obstetrics 25 years, others 8 years and so forth. This necessitates differential storage periods for records informed by attendance data and diagnosis from multiple patient information systems with the acute hospital setting in line with individual relevant patient event history.

Managing the retention and disposal of large volumes of records using such a complexity of data spread across multiple systems is hugely challenging, problematic and expensive. The Trust where necessary may therefore adopt a workable alternative lifecycle management strategy by identifying and archiving non-current records that do not have to be immediately or widely available based on when a record was last accessed.

6.5 Deletion/Disposal of Records

6.5.1 Identification of records for disposal is dependent upon accurate computer held patient 'last attendance' data on CareFlow EPR and correct application of procedures to facilitate extended retention if it is required.

6.5.2 Confidentiality must be fully maintained when records are destroyed. This is achieved by ensuring that all records for destruction are incinerated, shredded or digital data is irrecoverable. Where this service is provided by a contractor the methods used throughout all the stages (including transport for physical records) must provide satisfactory safeguards against accidental loss, disclosure or incomplete erasure.

6.6 Master Disposal Registers

The Trust will retain the Patient Master Index (PMI) as a master disposal register for shared Unit health records. The PMI will be retained permanently. Managers must use the Information Asset Register (IAR) to record retention and disposal of departmentally managed records and other IT systems.

6.7 Putting Information 'Beyond Use' where permanent deletion is not technically possible

6.7.1 Data protection legislation requires that information 'no longer required' should cease to be processed and either erase (delete) it, or anonymise it.. The Information Commissioner has consistently held that this means that reasonable steps should be taken to ensure the information is not retrievable by normal methods, normal in this case including restoring using back-up tapes etc.

There is a significant difference between permanently deleting personal data, and taking it offline. If personal data is stored offline, this should reduce its availability and the risk of misuse or mistake. However, we are still processing personal data. We should only store it offline (rather than delete it) if we can still justify holding it.

The word 'deletion' can mean different things in relation to electronic data, and we recognise it is not always possible to delete or erase all traces of the data. The key issue is to ensure you put the data beyond use. If it is appropriate to delete personal data from a live system, you should also delete it from any back-up of the information on that system.

Alternatively, you can anonymise the data so that it is no longer “in a form which permits identification of data subjects”.

Personal data that has been pseudonymised – eg key-coded – will usually still permit identification. Pseudonymisation can be a useful tool for compliance with other principles such as data minimisation and security, but the storage limitation principle still applies.

It is generally the view that removing the normal means of retrieval i.e. via the live environment, is sufficient to satisfy data protection in most environments provided that back-ups are also properly controlled to prevent them frustrating official retention policy.

For legacy systems - the relevant Information Asset Owner/Administrator must indicate how records will be put ‘beyond use’, e.g. via digital archiving, if they cannot be permanently deleted.

For new or upgraded systems - the relevant Information Asset Owner/Administrator should indicate via the Data Protection Impact Assessment, how digital held patient records will be deleted, or must explain why this is not technically feasible, and therefore must indicate how records will be put ‘beyond use’.

6.7.2 Subject Access Rights for Records put Beyond Use

The ICO does not require data controllers to grant individuals subject access to the personal data provided that all four safeguards above (6.7) are in place. Nor will they take any action over compliance with the fifth data protection principle. It is, however, important to note that where data put beyond use is still held; it might need to be provided in response to a court order and we must be prepared to respond to subject access requests for personal data stored offline, and must still comply with all the other principles and rights.

No patient records or data will be destroyed if it is the subject of a request under data protection legislation or any other legal process and this is brought to the attention of the Data Protection Officer by the Legal Team.

6.8 Extended Retention for Clinical, Legal or Research Purposes

In order to comply with data protection legislation, non-current records will not be preserved beyond the minimum preservation periods outlined unless there is a justifiable ‘case’ for their retention beyond those minimum periods and which that satisfy the requirements below.

The criteria for the retention of any patient identifiable record beyond the minimum periods are specifically:

I. that the records are required for research or other unspecified scientific purposes;
II. or that they are being retained in contemplation of proceedings against the Trust.

6.8.1 Clinical Purposes

Clinicians may apply to the Information Governance Committee (IGC) for particular records or record series to be retained for longer than the minimum periods set out in the Disposal Schedule. Such records may be kept on the basis that they meet the requirements set out in the appraisal procedure (See 6.11)

6.8.2 Legal Purposes

On the rare occasion it may be required the Legal Team will identify any records that require retention beyond the normal clinical retention period for use in conjunction with legal proceedings by adding an appropriate Medway Administrative Alert to act as a contra-indication to disposal. The practice prior to 2017 was to adhere a highly visible sticker to a records cover, after this date a Medway Administrative Alert is used.

6.8.3 Research Purposes

The Research and Innovation team are responsible for identifying health records of patients involved in studies by applying a visible sticker to the red “alert notification” page in health records. From 2016 onwards this is also detailed using the appropriate CareFlow EPR PAS alert recording ‘Clinical Research Status’.

6.8.4 Historical Context

There may be occasions where records or samples of records may be considered for permanent archival preservation and deposit e.g. examples of pioneering treatments. See 6.9.

6.9 Permanent Preservation of Paper and Digital Archives in Accordance with the Public Records Acts

6.9.1 It is a duty under the Public Records Act for the Trust to make appropriate arrangements for the selection and permanent preservation of public records within their control. That duty is subject to the provision that records of individual patients will not normally be preserved under the Public Records Act, other than by way of templates. The Trust has a selection process for this procedure.

6.9.2 The Information Governance Committee on behalf of the Trust, will from time to time, propose records that they deem suitable for permanent preservation as required by the Public Records Acts 1958 and 1967 and will recommend and offer them to a Place of Deposit approved by the National Archives who may accept or decline. Nottinghamshire Archives, County House, Castle Meadow Road, Nottingham, NG2 1AG are the current approved repositories for the Trust and its predecessor organisations.

6.9.3 Selection will be performed in consultation with health professionals, and archivists from the local Public Records place of deposit. If records are to be sampled, specialist advice must be sought from the same health professionals and archivists.

6.9.4 Once the Trust has made a selection decision, it is then incumbent upon the Trust to keep those records in its safe custody until such time that they can be transferred to the appointed Place of Deposit.

6.9.5 In accordance with the Public Records Act, the general public will not ordinarily have a right of access to deposited health records information linked to identifiable individuals for many decades, these are considered 'closed' records. However, places of deposit may contact the Trust in relation to requests from individuals to access information within closed records and each request will be assessed on an individual basis by either the Data Protection Officer or the Caldicott Guardian.

6.9.6 Potential transfers of digital archive material will need to be discussed with the Records Manager and the Place of Deposit to ensure technical and transfer issues are managed.

6.9.7 Approval must be sought from the Keeper of Public Records to retain records for more than 30 years after a patient's last contact with the Trust.

6.10 Extended or Permanent Retention - Application Process to Information Governance Committee

6.10.1 Applications for either extended or permanent retention of records require evaluation and approval from the Information Governance Committee. Further advice, including legal advice or that from the Information Governance team will be taken wherever necessary.

6.10.2 Applications must be made to Information Governance Committee using the standard Application/Appraisal Form (Appendix B of the Retention and Destruction Procedure available on the website[7]). The applicant must be able to identify each record concerned by D Number where it is the main identifier.

6.10.3 Implementation of this appraisal procedure for paper based records commenced in 2004. Prior to this, Consultants were given an opportunity to submit an application for extended or permanent preservation of records that would otherwise be disposed of under the auspices of the policy. Requests were submitted to the Health Records Management Group at the time for evaluation and approved or declined before policy implementation.

6.10.4 Records identified and agreed for extended or permanent preservation must remain in the safe custody of the Trust until disposal or transfer.

[7] https://www.sfh-tr.nhs.uk/about-us/policies-and-procedures/non-clinical-policies-procedures/information-governance/?id=8647

6.10.5 Records agreed for extended preservation may at any time be transferred to another media. e.g. scanned to a digital image.

6.10.6 A register of records approved for extended preservation at the Trust forms Appendix 4 of this policy.

6.10.7 From 2004 onwards the front covers of paper based health records approved for extended retention had to be clearly marked by the departments concerned using specific identification stamps/ stickers. The stickers acted as a visual contra-indication to disposal, this system will be superseded in future by use of appropriate PAS Alerts.

6.11 Information Governance Committee Appraisal Procedure

6.11.1 In considering individual applications the Information Governance Committee are obliged to use the following appraisal procedure as advocated by Records Management Code of Practice 2021, the advice of the Health Archives Group and the National Archives:

a) Consult with the relevant health professional body and clearly minute the actions;
b) consider any local clinical need; and
c) assess the value of the records for long-term research purposes/value, in consultation with Nottinghamshire Archives
d) Note existing precedents (the establishment of a continuity of selection).
e) Consider the historical context of records and the history of the institution (pioneering treatments and examples of excellence) within the context of its service to the local and wider community;
f) Ensure the provisions of the UK GDPR and Data Protection Act 2018 are complied with.

6.11.2 The outcome of an Information Governance Committee evaluation will set out a specific time period for extended preservation, the periods determined can be reviewable (‘extended’ preservation), or can immediately recommend ‘permanent’ preservation.

6.11.3 Information Governance Committee will consider and adopt the use of sampling techniques when it appears reasonable to keep only a percentage of records for particular reference.

Accountability

That adequate records are maintained to account fully and transparently for important actions and decisions, in particular:

- To protect legal and other rights of staff or those affected by those actions
- To facilitate audit or examination
- To provide credible and authoritative evidence if required by law.

Quality
That all records are periodically and routinely reviewed to determine what can be disposed of or destroyed. This will guarantee the quality of the records that are selected for permanent preservation.

Accessibility
That records which have been selected for archiving should be held in a repository that has been approved by The National Archives. This will guarantee appropriate conditions for storage and access.

Security
That the destruction of confidential records ensures that confidentiality is fully maintained. Currently a contractor provides this service, but it is the responsibility of the Trust to satisfy itself that the methods used throughout all stages, including transport to the destruction site, provide satisfactory safeguards against accidental loss or disclosure.

Papers and files containing confidential information must be disposed of in a secure manner and must not be disposed of with other domestic waste. Confidential waste consoles are provided throughout the Trust at all sites to dispose of confidential waste.

Medical records should be disposed of in line with appendix 4 of this policy.

Papers and files containing confidential information must be disposed of in a secure manner and must not be disposed of with other domestic waste.

Confidential waste must be held in a secure manner at all times prior to shredding, including the central disposal holding area.

Confidential waste such as un-shredded health records for destruction, nursing records, personal files etc., must be placed into the confidential waste consoles provided. Additional bags, if required in between collections, can be requested via the FM Helpdesk (3005), and arrangements made for them to be collected by portering staff via the FM Helpdesk (3005), quoting the room number of the secure location. No material other than paper is to be disposed of in the confidential waste stream.

Where departments wish to dispose of large quantities of confidential materials these should be planned in advance with the Waste Contract Manager to ensure that suitable containers are provided to facilitate removal.

A Certificate of Destruction will be obtained from the waste contractor by the Waste Contract Manager and retained.

Performance Measurement

That the application of retention and destruction of records procedures are regularly monitored against agreed indicators and action taken to improve standards as necessary.

Notes on preservation of health records for historical purposes

In light of the latest trends in medical and historical research, it may be appropriate to select some of these records for permanent preservation. Selection should be performed in consultation with health professionals and archivists from an appropriate place of deposit. If records are to be samples, specialist advice should be sought from the same health professionals and archivists. If an NHS Trust has taken on a leading role in the development of specialised treatments, then the patient records relating to these treatments may be especially worthy of permanent preservation. All records that make reference to historical child sexual abuse must be retained for permanent preservation.

If a whole run of patient records is not considered worthy of permanent preservation but nevertheless contains some material of research value, then the option of presenting these records to a local record office and other institutions under S.3(6) of The PRA should be considered. Advice on the presentation procedure may be obtained from the PRO's Archive Inspection Services.

If a whole run of patient records is considered worthy of permanent preservation but there is lack of space in the relevant place of deposit to store these records, contact the Information Governance Team who will advise on the most appropriate option available.

Any further advice requirement to implement this policy should be directed to the Information Governance Team.

Guidance on retention periods can be found under the Information Governance section on the staff intranet and Trust's website.

All digital and paper records that are selected for destruction must be recorded on the departments Destruction Log, an example of which can be found in Appendix 3. Destruction logs are audited as part of the annual Records Inventory.

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 (eg verbal, formal report etc) and by who)
Retention and Disposal Policy is Operational for Records registered as information assets	Information Governance Committee	Performance reporting of information assets appraisal and disposal	Bi-monthly	Standard performance report to Information Governance Committee
Reporting of any incidents involving inappropriate records disposal	Information Governance Committee	Performance reporting of IG incidents	Bi-monthly	Standard performance report to Information Governance Committee
Information Asset Owner report to the Senior Information Risk Owner (SIRO)	Information Asset Owner	Self-assessment return	Annually	Information Governance 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 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.[8]

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:

- Common law duty of confidentiality
- Data Protection Act 2018
- Freedom of Information Act 2000
- Freedom of Information Act Section 46 Code of Practice[9]
- Health and Social Care Act 2008
- Public Records Act 1958
- UK General Data Protection Regulation

[8] https://www.sfh-tr.nhs.uk/about-us/policies-and-procedures/non-clinical-policies-procedures/information-governance/

[9] https://ico.org.uk/media/for-organisations/documents/1624142/section-46-code-of-practice-records-management-foia-and-eir.pdf

- The key principles outlined within the policy in relation to disposal of records after scanning arise from the Civil Evidence Act 1995 and are supported in respect of criminal prosecutions by the Policy and Criminal Evidence Act 1984.

Accreditation:
- Care Quality Commission
- MHRA
- NHS England Data Security and Protection Toolkit

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 Procedure

11.0 KEYWORDS

Records management, Information Asset Owner, Information Asset Administrator, personal confidential data, Inquiry.

12.0 APPENDICES

- List of appendices are provided in the contents table.

APPENDIX 1 - EQUALITY IMPACT ASSESSMENT FORM (EQIA)

Name of service/policy/procedure being reviewed: Retention and Destruction Policy			
New or existing service/policy/procedure: Existing			
Date of Assessment: 13th January 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	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.	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
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?
None

What data or information did you use in support of this EqIA? Knowledge and experience
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? No
No

Level of impact
From the information provided above and following Equality Impact Assessment guidance on how to complete, the perceived level of impact is:

Low Level of Impact

Name of Responsible Person undertaking this assessment:
Gina Robinson

Signature:
Gina Robinson

Date:
23rd January 2025

APPENDIX 2 – ENVIRONMENTAL IMPACT ASSESSMENT

The purpose of an environmental impact assessment is to identify the environmental impact, assess the significance of the consequences and, if required, reduce and mitigate the effect by either, a) amend the policy b) implement mitigating actions.

Area of impact	Environmental Risk/Impacts to consider	Yes/No	Action Taken (where necessary)
Waste and materials	• Is the policy encouraging using more materials/supplies? • Is the policy likely to increase the waste produced? • Does the policy fail to utilise opportunities for introduction/replacement of materials that can be recycled?	Yes	
Soil/Land	• Is the policy likely to promote the use of substances dangerous to the land if released? (e.g. lubricants, liquid chemicals) • Does the policy fail to consider the need to provide adequate containment for these substances? (For example bunded containers, etc.)	No	
Water	• Is the policy likely to result in an increase of water usage? (estimate quantities) • Is the policy likely to result in water being polluted? (e.g. dangerous chemicals being introduced in the water) • Does the policy fail to include a mitigating procedure? (e.g. modify procedure to prevent water from being polluted; polluted water containment for adequate disposal)	No	
Air	• Is the policy likely to result in the introduction of procedures and equipment with resulting emissions to air? (For example use of a furnaces; combustion of fuels, emission or particles to the atmosphere, etc.) • Does the policy fail to include a procedure to mitigate the effects? • Does the policy fail to require compliance with the limits of emission imposed by the relevant regulations?	No	
Energy	• Does the policy result in an increase in energy consumption levels in SFHFT? (estimate quantities)	No	
Nuisances	• Would the policy result in the creation of nuisances such as noise or odour (for staff, patients, visitors, neighbours and other relevant stakeholders)?	No	

APPENDIX 3 - RECORDS DESTRUCTION LOG

Description of Record to be Destroyed	Electronic or Paper format	Owner/Department	Person Authorising Destruction	Retention Period	Date of Destruction
Email account for Joe Bloggs	Electronic	NHIS	Service Desk Manager	1 year	02.11.2010
Minutes of Health & Safety Committee	Paper	Human Resources	Assistant Director of HR	2 years	05.11.2010
Where relevant this should include the period that the documents cover – e.g. Supplier invoices for 2011/12					

APPENDIX 4 - RECORDS WITH APPROVED EXTENDED RETENTION

Directorate	Responsible Clinician/Applicant	Date of application	Details of extended preservation
Corporate	Lee Radford	13th November 2020	Work experience/work placements records. To be destroyed after for 7 financial years
Trust wide		4th June 2024	Health records - to be destroyed 30 years after last attendance and 10 years after death.
Trust wide	Occupational health records	17th January 2025	Classed as a major record, however no defined rules in the Code of Practice.

Occupational Health records

Individual aged over 75s?	Yes	Review record contents to determine if for destruction or retention	Staff Member still employed by SFH	Paper records to be scanned to OPAS G2 for digital storage until termination of employment date + 6 years.
			No longer employed with **NO** Health Surveillance Records	Record to be securely destroyed and details of destruction logged.
			No Longer employed **WITH** Health Surveillance Records	Paper records to be scanned to OPAS G2 for digital storage until relevant retention period expires (75 years of age for Spirometry and Audiometry, 50 years since last entry OR 75 years old whichever is longer for ionising radiation medicals)
	No		File by year of birth and keep record in review cycle until 75 years of age.	