NHS
Yorkshire
Ambulance Service
NHS Trust

Records Management Policy

Document Author: Head of Risk and Assurance

Date Approved: August 2023

Document Reference	PO – Records Management Policy
Version	12.0
Responsible Committee	Trust Management Group
Responsible Director (title)	Executive Director of Quality, Governance and Performance Assurance
Document Author (title)	Head of Risk and Assurance
Approved by	Trust Management Group
Date Approved	August 2023
Review Date	August 2025
Equality Impact Assessed (EIA)	Yes - Screening
Protective Marking	Not protectively marked.

Document Control Information

Version	Date	Author	Status (A/D)	Description of Change
2.0	Sept 2008	David Johnson	A	Revisions to format and content.
3.0	Feb 2010	David Johnson	A	Revisions to format and content.
4.0	Feb 2011	David Johnson	A	Revisions to format and content. Amended staff details in table, section 14.10.
5.0	Dec 2011	Julie Barber	A	Revisions to format and content. Updated to reflect minor changes in processes/procedures and policy over the last 12 months.
5.1	Feb 2013	Caroline Squires	D	Significant revisions to existing procedural document in relation to content and format.
5.2	April 2013	Caroline Squires	D	Minor amendments following consultation with Information Governance Working Group members.
5.3	May 2013	Caroline Squires	D	Amendments to content and format following Senior Management Group meeting.
6.0	June 2013	Caroline Squires	A	Minor amendments. Approval by Senior Management Group.
6.1	Nov 2015	Caroline Squires	D	Amendments to reflect latest policy format and minor accuracy changes.
7.0	Dec 2015	Caroline Squires	A	Approval by Trust Management Group in December 2015.
7.1	Dec 2016	Leon Kaplan	D	Amendments to reflect Records Management Code of Practice 2016
8.0	Feb 2017	Leon Kaplan	A	Approved by TMG
8.1	Sept 2017	Allan Darby	A	Extension agreed at TMG in preparedness for the launch of General Data Protection Regulations which come in to force May 2018. IG policies remain best practice up to this date.
8.2	Apr 2018	Allan Darby	D	Amended to reflect GDPR and Data Security and Protection Toolkit requirements.
8.3	April 2018	Risk Team	D	New Visual Identity – Document Formatted
	April 2018	IG Working Group		Review by IG Working group – agreed
9.0	May 2018		A	TMG – approved subject to adding a paragraph regarding loss of paper PCRs – completed at 3.5

9.1	August 2020	Ruth Parker	D	Date agreed by TMG for review date extension
9.2	Feb 2021	Head of Risk and Assurance	D	Full review
10.0	May 2021	Risk Team	A	Approved at TMG
10.1	Sept 2021		D	Amendment made to retention schedule to reflect the new Records Management Code of Practice
11.0	Nov 2021	Risk Team	A	Approved at TMG
11.1	Aug 2023	Head of Risk and Assurance	D	• Minor grammar amendments made throughout • Removal/Amendments of named documents in ‘Associated Documentation’ • Goddard Enquiry information now removed as this is now completed. • Addition of wording in retention doc under ‘Invoices’ • Clinical Trials link amended. • Amendment made to 1.3 • Grammatical changes made
12.0	August 2023	Head of Risk & Assurance	A	Approved at IG Working Group

A = Approved D = Draft

Document Lead = Head of Risk and Assurance

Associated Documentation:

Data Protection Policy
Information Governance Framework
Information Sharing Policy

Data Quality Policy
Disclosure Policy
Freedom of Information Policy
ICT Security Policy and Associated Procedures
Email Policy
Internet Policy and Procedure
Social Media Policy
Safety and Security Policy
Incident and Serious Incident Management Policy
Surveillance Camera Systems Policy
Safeguarding Policy
Disciplinary Policy and Procedure
YAS Code of Conduct

Staff Summary

Records Management is the process by which an organisation manages all the aspects of records, whether internally or externally generated, and in any format (paper or electronic) or media type, from their creation, all the way through their lifecycle, to their disposal or permanent archive.
The Trust's records are its corporate memory, providing evidence of actions and decisions and representing a vital asset to support daily functions and operations.
The Trust is committed to on-going improvement of its records management functions as it believes that it will gain a number of organisational benefits from doing so.
This policy supports at a local level the legal and best practice requirements set out with the Records Management Code of Practice for Health and Social Care for those who work within or under contract to NHS organisations in England, based on current legal requirements and professional best practice.
All NHS records are Public Records under the Public Records Acts.
All records (paper or electronic) containing personal data are covered by the UK General Data Protection Regulations (GDPR) 2020 and the Data Protection Act 2018 and consequently the provisions of the Act apply to all of the Trust's records containing personally identifiable information including patient and staff records.
All staff must ensure that high standards of data quality are applied at every phase of the records lifecycle.
The security of all Trust records is critical, as records provide evidence of business transactions, support management decisions and ensure public accountability requirements are met.
The retention period varies dependent on the type of information being stored.
Disposal is defined as the point in the records lifecycle when it is either transferred to an archive, or securely destroyed.

1.0 Introduction

1.1 Records Management is the process by which an organisation manages all the aspects of records, whether internally or externally generated, and in any format (paper or electronic) or media type (see 1.3 below), from their creation, all the way through their lifecycle, to their disposal or permanent archive.

1.2 The Trust's records are its corporate memory, providing evidence of actions and decisions and representing a vital asset to support daily functions and operations. Records support policy formation and managerial decision-making, protect the interests of the Trust and the rights of patients, staff and members of the public. They support consistency, continuity, efficiency and productivity and help deliver services in consistent and equitable ways. Records are required for a number of reasons and are essential to the organisation. Some examples of why records are needed are detailed below:

- To support patient care and continuity of care.
- To support the day-to-day business and the delivery of care.
- To support evidence based clinical practice.
- To support sound administrative and managerial decision making, as part of the knowledge base for NHS services.
- To meet legal requirements, including requests from patients under subject access provisions of the UK General Data Protection Regulation, Data Protection Act and/or the Freedom of Information Act.
- To assist clinical and other types of audits.
- To support improvements in clinical effectiveness through research and also to support archival functions by taking account of the historical importance of material and the needs of future research.
- To support patient choice and control over treatment and services designed around patients.
- To support regulatory activities and processes such as investigations, inquiries and inspections

1.3 Examples of types of record and media covered by this policy include:

- Patient clinical records (paper or electronic).
- Integrated health and social care records.
- Data processed for secondary use purposes. Secondary use is any use of person level or aggregate level data that is for direct care purposes. This can include data for service management, research or support for commissioning.
- Corporate records (such as HR, estates, financial, complaint-handling, committee papers).
- Photographs and other visual images.
- Audio and video tapes, CDs etc.
- Emails.

- Computerised records.
- Scanned records.
- SMS text messages (both outgoing from the NHS and incoming responses), and other forms of messages such as Messenger and What's App.
- Material intended for short term or transitory use, including notes and copies of documents.
- Websites and intranets sites that provide key information for patients and staff.

1.4 The Trust is committed to on-going improvement of its records management functions as it believes that it will gain a number of organisational benefits from doing so. These include:

- Better use of physical and digital space.
- Clear standards for record keeping, tracking and destruction.
- Better use of staff time and more efficient workflows.
- Improved control, access, and retrieval of valuable information assets.
- Compliance with legislation and professional standards.
- Reduced business costs resulting from poor records management.
- Reduced volume of lost or duplicated information.
- A better understanding of the types of records held.
- An informed and educated workforce, able effectively to carry out records management responsibilities.

2.0 Purpose/Scope

2.1 The purpose of this policy is to provide clear guidance to all staff in the handling and management of all records, both corporate and clinical, regardless of the media on which they are stored. Additionally, this policy sets out a framework within which staff responsible for managing the Trust's records can develop specific local procedures to ensure that records are managed and controlled effectively commensurate with legal, operational and information needs.

2.2 This policy supports at a local level the legal and best practice requirements set out with the Records Management Code of Practice for Health and Social Care for those who work within or under contract to NHS organisations in England, based on current legal requirements and professional best practice. This has been published by the Information Governance Alliance (Department of Health, NHS England, NHS Digital, and Public Health England).

2.3 All staff are personally responsible for making themselves aware of and complying with this policy.

3.0 Process

3.1 Legal and Regulatory Obligations

3.1.1 All NHS records are Public Records under the Public Records Acts. The Trust will take action as necessary to comply with the legal and professional obligations set out in the Records Management Code of Practice for Health and Social Care, in particular:

- The Public Records Acts 1958 and 1967.
- UK General Data Protection Regulation (GDPR) 2020.
- Data Protection Act 2018.
- The Freedom of Information Act 2000.
- Lord Chancellor's Code of Practice on the Management of Records issued under section 46 of the Freedom of Information Act 2000 which directs public organisations to have records management systems which will help them perform their statutory function.
- The Common Law Duty of Confidentiality.
- The NHS Confidentiality Code of Practice; and
- Any new legislation affecting records management as it arises.

3.1.2 All records (paper or electronic) containing personal data are covered by the UK General Data Protection Regulation (GDPR) 2020 and the Data Protection Act 2018 and consequently the provisions of the Act apply to all of the Trust's records containing personally identifiable information including patient and staff records.

3.1.3 For most health professionals, there are relevant codes of practice issued by the registration bodies and membership organisations of staff. That guidance is designed to guard against professional misconduct and to provide high quality care in line with the professional bodies.

3.1.4 The Academy of Medical Royal Colleges (AoMRC) has 12 generic medical record keeping standards.

3.1.5 There is professional guidance on the structure and content of the clinical records of ambulance patients, hosted by the Royal College of Physicians.

3.2 Records Creation, Capture, Maintenance and Quality

3.2.1 **Record Creation**

When creating information in the first instance, these principles apply:

- ***Available when needed*** - to enable a reconstruction of activities or events that have taken place.
- ***Accessible to all members of staff that require access in order to enable them to carry out their day-to-day work*** - the information must be

located and displayed in a way consistent with its initial use and that the current version is clearly identified where multiple versions exist.

- ***Interpretable, clear and concise*** - the context of the information must be clear and be able to be interpreted appropriately, i.e., who created or added to the record and when, during which business process, and how the record is related to other records. This is especially important for managing emails.[1]
- ***Trusted, accurate and relevant*** - the information must reliably represent the initial data that was actually used in, or created by, the business process whilst maintaining its integrity. The authenticity must be demonstrable and the content relevant.
- ***Secure*** - the information must be secure from unauthorised or inadvertent alteration or erasure. Access and disclosure must be properly controlled, and audit trails used to track all use and changes. The information must be held in a robust format which remains readable for as long as the information is required or retained.

Employees should also consider the following when creating information for the first time:

- What is being recorded and how it should be recorded.
- Why is it being recorded.
- How to validate the information (and against what) in order to ensure that what is being recorded is the correct data.
- How to identify errors and how to report errors and correct them accordingly.
- The intended use of the information; understand what the records are used for (and therefore why timeliness, accuracy and completeness of recording is so important).
- How to update the information and how to add in information from other sources.

3.2.2 Record Capture

For reasons of business efficiency or in order to address problems with storage, consideration should be given to the option of scanning paper records into electronic format. Where this is proposed, the factors to be taken into account include the:

[1] Email fixes information in time and assigns an action to an individual, which are two of the most important characteristics of an authentic record. However, a common problem with email is that it is rarely saved in the business context, which is the third characteristic to achieve an authentic record. The correct place to store email is in the record keeping system of the activity to which it relates. If an email is declared as a record, or as a component of a record, the entire email must be kept including attachments so the record remains integral, e.g., an email approving a business case must be saved with the business case file.

- Costs of the initial (and any later) media conversion to the required standard, bearing in mind the length of the retention period for which the records are required to be kept.
- Need to consult in advance with the local Place of Deposit or The National Archives with regard to records which may have archival value, as the value may include the format in which it was created.
- Need to protect the evidential value of the record by copying and storing the record in accordance with British Standards, in particular the ‘BS 10008 Electronic Information Management – Ensuring the authenticity and integrity of electronic information’.
- In order to fully realise the benefits of reduced storage requirements and business efficiency, the Information Asset Owners (IAOs) should dispose of any paper records that have been copied into electronic format and stored in accordance with appropriate standards. Where the record constitutes confidential information, it must be securely destroyed.

3.2.3 Record Maintenance

All information needs to be maintainable through time. The qualities of availability, accessibility, interpretation and trustworthiness must be maintained for as long as the information is needed (perhaps permanently), despite changes in the format.

3.2.4 Record Quality

All staff must ensure that high standards of data quality are applied at every phase of the records lifecycle; for further detailed guidance please refer to the Data Quality Policy.

3.3 Records Use - Control, Tracking, Security and Storage

3.3.1 Record Control

The use of standardised file names and version control methods should be applied consistently throughout all record lifecycles. Please refer to the table below for guidance on how to version control a document from the point of its creation, on-going maintenance and throughout its use.

How to Version Control a Document

Stage	Version Number	Filename
Initial creation	0.1	APolicyDocument_v0.1 - draft
Second draft to include some feedback	0.2	APolicyDocument_v0.2 - draft
Third draft to include changes from stakeholders	0.3	APolicyDocument_v0.3 - draft
All changes included, ready for approval	0.4	APolicyDocument_v0.4 - draft

Approved version – now ready for release	1.0	APolicyDocument_v1.0 - FINAL
DOCUMENT PUBLISHED AND RELEASED	**1.0**	APolicyDocument_v**1.0** - **FINAL**
Review now due		
Make amendments on the draft as applicable	1.1	APolicyDocument_v1.1 - draft
Incorporate feedback from stakeholders	1.2	APolicyDocument_v1.2 - draft
Issue for approval	1.3	APolicyDocument_v1.3 - draft
Incorporate feedback from the approvers	1.4	APolicyDocument_v1.4 - draft
Re-issue for final approval	1.5	APolicyDocument_v1.5 - draft
Approved version – now ready for release	2.0	APolicyDocument_v2.0 - FINAL
DOCUMENT RE-PUBLISHED AND RE-RELEASED	**2.0**	APolicyDocument_v**2.0** - **FINAL**

Where possible all staff must avoid duplication and printing copies of records. This increases risks of breaches of confidentiality and needlessly increases administrative and paper costs felt by the Trust. Where the creation of copies is unavoidable, they must be destroyed as soon as they are no longer required.

3.3.2 Tracking Electronic Records

The tracking of electronic records is held automatically in the audit trails of the systems that hold the data.

Best practice is to ensure version control is always applied as a minimum. If a particular record cannot be version controlled, has no automatic system audit trail and a manual audit trail cannot be easily applied directly to the record itself, consideration should be given to a separate document that details the audit of amendments to that particular record.

3.3.3 Tracking Paper Records

Paper records do not have the facility of an automatic audit trail that electronic systems offer and so staff must enter a manual audit trail in the record itself that details the full name of the person to last update the record and the date and time the amendment was carried out.

Depending on the nature of the record, this level of detail may not always be applicable, however best practice is to ensure version control is always applied as a minimum. If a particular record cannot be version controlled and a manual audit trail cannot be easily applied directly to the record itself, consideration should be given to a separate document that details the audit of amendments to that particular record.

Whilst the organisation is continually making changes to help reduce the amount of paper records produced in the first instance and to also convert some existing paper-based records into electronic format using scanning, there is always likely to be the need for some paper-based records within the organisation. In the first instance, staff must always look for alternative methods of creating, storing and maintaining records that do not involve the paper-based means being the primary source. However, where a suitable electronic alternative is not readily available, staff must always seek to be as efficient as possible, file records in a logical manner to aid future retrieval and avoid making unnecessary duplications to help reduce the risk of data being lost, or unlawfully disclosed.

3.3.4 **Record Security and Storage**

The security of all Trust records is critical, as records provide evidence of business transactions, support management decisions and ensure public accountability requirements are met. Records in all formats should be stored securely to prevent unauthorised access, destruction, alteration or removal. Trust staff are responsible for the safe custody of all files and documents.

No paper records can be taken off Trust premises, e.g., home, except for a temporary period (i.e., overnight or at most a weekend), where a member of staff's travel to a meeting requires this. In all cases, only the minimum number of records relevant to that meeting is permitted. The member of staff must ensure the safe storage of those records whilst in their personal possession. The records must be returned to Trust premises by the next working day.

Paper records that are sensitive or hold confidential information should be placed in a secure storage area when not in use. Paper records must be stored in secure and preferably alarmed facilities with strict access controls in place. Electronic records must be protected at all times from unauthorised disclosure, access and corruption.

Storage of records in offices must conform to all current relevant legislation and guidance regarding Health and Safety, namely the Health & Safety at Work Act 1974 and Workplace (Health, Safety and Welfare) Regulations 1992. Records held in offices are generally those that are in current use. These records must be securely stored to prevent theft or unauthorised access.

Offsite storage areas must conform to all current relevant legislation and guidance regarding Health and Safety, namely the Health & Safety at Work Act 1974 and Workplace (Health, Safety and Welfare) Regulations 1992. The Trust has a contract with an external supplier to provide secure storage of archive records. All records stored off site must still comply with retention periods.

The Trust follows the protective marking scheme for patient information as being 'NHS Confidential', which corresponds to the classification of "Official

Sensitive" under the Cabinet Office Government Security Classifications (2014).

3.4 Records Retention, Appraisal and Disposal

3.4.1 Records Retention

The table in Appendix C details the minimum retention period for each type of record.

The retention period varies dependent on the type of information being stored. The information being recorded and retained must be relevant, fit for the purpose it was intended, and only retained for as long as it is genuinely required.

3.4.2 Records Appraisal

The process of deciding what to do with records when their business use has ceased is called appraisal. The three outcomes of appraisal are: destroy/delete (see 3.4.3 below); keep for a longer period (see 3.4.1 above) or transfer to a place of deposit appointed under the Public Records Act 1958 (see 3.5 below).

3.4.3 Records Disposal

Disposal is defined as the point in the records lifecycle when it is either transferred to an archive, or securely destroyed. It is particularly important under the Freedom of Information legislation that the disposal of records is undertaken in accordance with this policy and in accordance with the retention requirements of any local and national inquiries such as the Independent Inquiry into Child Sex Abuse (IICSA) Local guidance should be followed in relation to record retention instructions issued by inquiries.

No record should be destroyed until the retention period for that particular record type has expired. The retention periods for the most frequently used record types are listed in the table in Appendix C.

Records believed to be ready for destruction should be documented onto the form '**Authorisation for Destruction of YAS Records**', which can be provided by the Information Governance Team.

Once all the details of the records that need destroying have been listed, the relevant Executive Director / Associate Director must authorise the destruction. At no point should any member of staff request destruction of any records without the signed permission of a Director / Associate Director. This authorisation process should be used for records held locally on YAS premises as well as records held by the Trust's records storage contractor, and the authorisation process should be used irrespective of whether the record is of a confidential nature or not.

The destruction exercise relating to records held by the records storage contractor will be co-ordinated by the Information Governance Team in conjunction with the relevant Information Asset Owners (IAOs).

Confidential paper-based records held locally on YAS premises must be securely disposed of as soon as possible after they are eligible.

3.5 Records Archiving

3.5.1 Records of the NHS and its predecessor bodies are subject to the Public Records Act 1958, which imposes a statutory duty of care directly upon all individuals who have direct responsibility for any such records. If the records have no on-going administrative value but have or may have long-term historical or research value, they may be more appropriately held as archives. Records with such value must be transferred to the organisation's approved Place of Deposit. Where the organisation has no existing relationship with a Place of Deposit, The National Archives should be contacted in the first instance. Where the Trust is unsure whether records may have archival value, The National Archives or the Place of Deposit with which the organisation has an existing working relationship should be consulted.

3.5.2 It is a legal requirement that NHS records which have been selected as archives should be held in a repository that has been approved for the purpose by The National Archives (TNA). Where an organisation is already in regular contact with its Place of Deposit, it should consult with it over decisions regarding selection and transfer of records. Where this is not the case, TNA should be contacted in the first instance.

3.6 Records Transfer

3.6.1 The mechanisms for transferring records from one organisation to another should be tailored to the sensitivity of the material contained within the records and the media on which they are held. Before transferring any information that may be of a confidential nature you must have approval from the relevant IAO for the business area concerned.

3.6.2 Ensure that all transfers of confidential records are handled in accordance with the Trust's:

- Data Protection Policy.
- ICT Security Policy and Associated Procedures.
- Disclosure Policy; and
- Email Policy.

3.7 Records Access, Retrieval and Disclosure

3.7.1 Records Access

Records must be available to all authorised staff who require access to them for business purposes.

Records held in electronic format are often easier to access and maintain, however staff must always ensure that records are not being accessed unnecessarily or kept for any longer than reasonably required just because it is easier to do so. If the records contain information that is personally identifiable the principles of the UK General Data Protection Regulations (GDPR) 2020 and the Data Protection Act 2018, as well as the Caldicott Principles, must be adhered to.

Records held in paper format are less easy to access, maintain and control than electronic records due to the very nature of them. Paper based records often only have the one master copy and are difficult to back up easily and cost effectively. Therefore, staff must take additional precautions when safeguarding and filing paper records to ensure that retrievals will be possible, when required at some point in the future. Where possible the filing and archiving of paper-based records should provide sufficient information to allow the identification of the records needed and wherever possible should be filed in accordance with the intended future destruction date, i.e., all records due to be destroyed on the same date should be filed together. This makes the secure destruction of these records much more straight forward.

3.7.2 Records Retrieval

All electronic corporate/business records should be stored on SharePoint or One Drive, which are regularly backed up, and not on the C drives of Trust computers, laptops or peripheral devices. This enables the retrieval of information by staff other than the author where appropriate and necessary. It also greatly reduces the risk of loss due to the failure of laptop or desktop PC hard drives or theft.

The retrieval of electronic records is also easier to control due to the rights and restrictions that can automatically be applied to individual staff logins for the various systems that hold records. Managers are responsible for authorising and requesting the appropriate user rights for individual members of staff, however all staff continue to be responsible for the security and integrity of the records and information which they record, handle, store, or otherwise come across during their day-to-day duties.

All information must be used consistently, only for the purpose for which it was intended, and never for an individual employee’s personal gain or purpose. If in doubt employees should seek guidance from the Information Governance Team in the first instance, who will inform the relevant IAO for the business area concerned.

3.7.3 Retrieving Archived Paper Records held in Storage with External Storage Contractor

To retrieve archived paper records that have been boxed and stored with the organisation’s external storage contractor, please contact the Information Governance Team.

3.7.4 Records Disclosure

Personally identifiable information held on corporate/business records must be treated as strictly confidential and may only be disclosed to individuals authorised as part of their day-to-day work to have access to it, or with the written consent of the person in question. There are exceptions where disclosure may be permitted, please refer to the Trust's Disclosure Policy and the Legal Services Department for further advice.

3.8 Requests for Information by External Third Parties

3.8.1 Should members of staff be approached by a third-party organisation for copies of any information they must refer the request to the appropriate team within the organisation. Under no circumstances should staff divulge any information, however small, to anyone external to the organisation.

3.8.2 Staff must direct all such requests immediately to the teams trained to handle and process these requests or, alternatively, seek advice and support from their line manager in the appropriate direction of the request. The majority of requests will be handled by the Legal Services Department who will take ownership of the request and ensure that it is handled in a consistent manner, whilst also ensuring that any disclosures of personally identifiable information are in strict accordance with the Data Protection Act 2018 and Common Law Duty of Confidentiality. The Safeguarding Team and Human Resources Team also handle requests for information in certain circumstances.

3.8.3 The requests may be, but are not limited to, Subject Access Requests, Police and Coroners' requests or any other type of request where staff are asked for copies of ePR/PCR forms, copies of calls placed with the Emergency Operations Centre (EOC) and any other documentation held by the organisation. Requests may also originate from registrant bodies such as the HCPC or from other Trusts for information pertaining to internal investigations.

3.9 Requests for Information by Internal Trust Staff

3.9.1 Should staff be approached to provide copies of records, divulge information verbally or confirm specific details of records to internal Trust staff, this is acceptable providing the member of staff being approached is confident that the person requesting the information is actually a member of Trust staff and the Caldicott Principles are followed at all times, specifically the 'need to know' principle. Should the staff member be in any doubt, it is acceptable to ask for the request to be emailed in order to verify the requesting staff member's identity and the legitimacy of the request. If there is any doubt following the email request, then staff should discuss the request with their line manager the Information Governance Team before disclosing any information.

3.9.2 For full details on the procedures for handling requests for information by external third parties and/or internal Trust staff, please refer to the Disclosure Policy.

4.0 Training Expectations for Staff

Training is delivered as specified within the Trust Training Needs Analysis (TNA).

5.0 Implementation Plan

The latest approved version of this policy will be posted on the Trust Intranet site for all members of staff to view. New members of staff will be signposted to how to find and access this policy and associated procedures during Trust Induction.

6.0 Monitoring Compliance with this Policy

A variety of methods will be used for monitoring compliance against the Records Management Policy including, confidentiality audits and risk reviews to be carried out by IAOs.

Failure to comply with this policy may result in disciplinary action being taken.

7.0 Appendices

Appendix A: Definitions

Personal Data	Personal Data is any information relating to natural persons: • who can be identified or who are identifiable, directly from the information in question; or • who can be indirectly identified from that information in combination with other information.
Special Categories of Data	Special Categories of Data is any personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, or data concerning a person's sex life or sexual orientation.
Data Controller	The entity that, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data Processor	An entity that processes data on behalf of, and only on the instructions of, the relevant Data Controller.
Data Subject	Any natural person whose personal data is processed by a controller or processor.
Processing	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Third Party	Any individual/organisation other than the data subject, the data controller (the Trust) or its agents.
Consent	Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
Healthcare Purposes	Includes all activities that directly contribute to the diagnosis, care and treatment of an individual and the audit/assurance of the quality of the healthcare provided. Does not include research, teaching, financial audit and other management activities.
Anonymised Data	Information which does not relate to an identified or identifiable natural person.

Pseudonymisation	The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Appendix B: Roles & Responsibilities

Chief Executive

As the accountable officer for the Trust, the Chief Executive has overall responsibility for compliance with the UK GDPR and Data Protection Act 2018. Operational responsibility for data protection is delegated to the Senior Information Risk Owner (SIRO), Data Protection Officer and all Information Asset Owners (IAOs).

Senior Information Risk Owner (SIRO)

The Board-level SIRO, under delegated authority from the Chief Executive, oversees compliance with the Data Protection Act and is responsible for the Trust's information risk. The Trust's SIRO is the Executive Director of Quality, Governance and Performance Assurance. The SIRO is supported by the Data Protection Officer, Information Asset Owners, and Information Governance Team.

Caldicott Guardian

The Caldicott Guardian is responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing. The Caldicott Guardian is responsible for providing advice within the Trust on the lawful and ethical processing of patient information. The Executive Medical Director acts as the Trust's Caldicott Guardian and is supported on a day-to-day basis by the Deputy Medical Director who plays a key role in ensuring that the organisation satisfies the highest practicable standards for handling patient identifiable information.

Data Protection Officer (DPO)

A Data Protection Officer (DPO) is a role mandated for public bodies, for organisations carrying out regular and systematic monitoring of data subjects on a large scale, and for organisations carrying out large scale processing of special category data (e.g., health and social care) or criminal convictions data. The Head of Risk and Assurance acts as the Trust's DPO and is supported on a day-to-day basis by the Information Governance Team. The DPO advises the organisation on data protection matters, monitors compliance and is a point of contact on data protection for the public and the ICO.

Associate Director of Performance Assurance and Risk

The Associate Director of Performance Assurance and Risk on behalf of the Trust Board is responsible for the ongoing delivery of this policy/framework. He/she will provide regular reports to the Risk and Assurance Group (RAG) on progress against its implementation.

Risk and Assurance Group (RAG)

This policy/framework will be overseen by the Risk and Assurance Group (RAG), chaired by the Associate Director of Performance Assurance and Risk. This group will receive assurance of ongoing progress against the policy/framework.

Trust Management Group

The Trust Management Group, chaired by the Chief Executive, will receive policies and proposals for approval.

Information Governance Team

The Information Governance Team provides day-day-day operational support to the SIRO and Caldicott Guardian and is responsible for providing general advice and guidance on data protection and the application of this policy.

Information Asset Owners (IAOs)

The SIRO is supported by a network of Information Asset Owners (IAOs) and Information Asset Administrators (IAAs). These individuals are responsible for interpreting information governance policy, applying it on a practical level within their area of responsibility and ensuring that policies and procedures are followed by staff. They recognise actual or potential security incidents, consult with the SIRO and Caldicott Guardian in relation to incident management and ensure that ROPA are accurate and up to date.

Information Governance Working Group (IGWG)

The Information Governance Working Group (IGWG) consists of all Information Asset Owners (IAOs).

All Staff

All staff are responsible for making sure they have read and understood this policy and associated procedures and are aware of the disciplinary and legal action that could potentially be taken if this policy and associated procedures are not followed. Compliance with data protection legislation is the responsibility of all members of staff including anyone providing a service on behalf of the Trust.

Appendix C: Retention Periods for each Record Type

The Records Management Code of Practice for Health and Social Care sets out what people working with or in NHS organisations in England need to do to manage records correctly. It's based on current legal requirements and professional best practice and was published by the Information Governance Alliance (IGA).

Appendix II of the Code contains the detailed retention schedules. It sets out how long records should be retained, either due to their ongoing administrative value or as a result of statutory requirement. The table below does not contain all record types covered in the Code and detailed retention schedules, only those records that are used or referred to most frequently in the Trust have been extracted for guidance. If information is required regarding another type of record not listed in the table, please refer to the Code of Practice and the detailed retention schedules.

1. Care Records with standard retention periods

Record Type	Retention period	Action at end of retention period	Notes
Adult health records not covered by any other section in this schedule	8 years	Review and consider transfer to PoD	Records involving pioneering or innovative treatment may have archival value, and their long-term preservation should be discussed with the local PoD or The National Archives.
Children's records Children's records (including midwifery, health visiting and school nursing) - can include medical illustrations, as well as video and audio formats.	25th or 26th birthday (see Notes)	Review and if no longer needed destroy	Retain until 25th birthday, or 26th if the patient was 17 when treatment ended.

Record Type	Retention period	Action at end of retention period	Notes
Electronic Patient Records System (EPR)	See Notes	Review and destroy if no longer required	Where the system has the capacity to destroy records in line with the retention schedule, and where a metadata stub can remain demonstrating that a record has been destroyed, then the Code should be followed in the same way for electronic records as for paper records with a log being kept of the records destroyed. If the EPR does not have this capacity, then once the records have reached the end of their retention period, they should be made inaccessible to system users upon decommissioning. The system (along with audit trails) should be retained for the retention period of the last entry related to the schedule.

2. Pharmacy

The IGA are conducting further work to expand this section which will be updated in the near future. As an interim measure you can view a list of Pharmacy records and their associated retention periods and actions by clicking on this link to the NHS East and South East Specialist Pharmacy Services retention schedule

Record Type	Retention period	Action at end of retention period	Notes
Controlled Drugs Registers	2 years See Notes	Review and if no longer needed destroy	Misuse of Drugs Act 2001. NHS England has issued guidance in relation to controlled drugs.
Controlled Drugs – order books, requisitions etc.	2 years	Review and destroy if no longer required	Misuse of Drugs Act 2001

3. Event & Transaction Records

Record Type	Retention period	Action at end of retention period	Notes
Clinical Audit	5 years	Review and if no longer needed destroy	Five years from the year in which the audit was conducted. This includes the reports and data collection sheets/exercise. The data itself will usually be clinical so should be kept for the appropriate retention period, for example, data from adult health records would be kept for 8 years.
Clinical Protocols	20 years	Review and consider transfer to a Place of Deposit	Clinical protocols may have preservational value. They may also be routinely captured in clinical governance meetings which may form part of the permanent record (refer to corporate governance records).
Destruction certificates, or electronic metadata destruction stub, or record of clinical information held on physical media	20 years	Review and consider transfer to a Place of Deposit	Destruction certificates created by public bodies are not covered by a retention instrument (if they do not relate to patient care and if a PoD or The National Archives do not accession them). They need to be destroyed after 20 years.
Equipment maintenance logs	11 years	Review and destroy and no longer required	
Inspection of equipment records	11 years	Review and destroy and no longer required	

Notifiable disease book	6 years	Review and destroy and no longer required	
Patient Property Books	2 years	Review and destroy and no longer required	Two years from the end of the year to which they relate.

4. Telephony Systems & Services (999 phone numbers,111 phone numbers, ambulance, out of hours, single point of contact call centres).			
Record Type	**Retention period**	**Action at end of retention period**	**Notes**
Recorded conversations – which may be needed later for clinical negligence or other legal purposes	6 years	Review and destroy if no longer required	Retention period runs from the date of the call and is intended to cover the Limitation Act 1980. Further guidance is issued by. https://resolution.nhs.uk/
Recorded conversation which forms part of the health record	Treat as a Health Record	Review and if no longer needed destroy	It is advisable to transfer any relevant information into the main record through transcription or summarisation. Call handlers may perform this task as part of the call. Where it is not possible to transfer clinical information from the recording to the record the recording must be considered as part ofthe record and be retained accordingly. See Adult or Children Health records.
Telephony Systems Record	1 year	Review and destroy if no longer required	This is the minimum specified to meet NHS contractual requirements.

5. Clinical Trials & Research

For clinical trials record retention please see the MHRA guidance at The Medicines for Human Use (Clinical Trials) Amendment Regulations 2006 (legislation.gov.uk)

Record Type	Retention period	Action at end of retention period	Notes
Clinical trials – applications for ethical approval	5 years	Review and consider transfer to a Place of Deposit	Master file of a trial authorised under the European portal, under Regulation 536/2014. For clinical trials records retention refer to the MHRA guidance. The sponsor of the study will be the primary holder of the study file and associated data. This is based on the Medicines for Human Use (Clinical Trials) Amendment Regulations 2006 (specifically Regulations 18 and 28).
Research data sets	No longer than 20 years	Review and consider transfer to a Place of Deposit	
Research – ethics committee's and HRA approval documentation for research proposal and records to process patient information without consent.	5 years	Review and consider transfer to a Place of Deposit	This applies to trials where opinions are given to proceed with the trial, or not to proceed. These may also have archival value.

Research – ethics committee’s minutes (including records to process patient information without consent)	20 years	Review and consider transfer to a Place of Deposit	Retention period begins from the year to which they relate and can be as long as 20 years. Committee minutes must be transferred to PoD.

6. Corporate Governance

Record Type	Retention period	Action at end of retention period	Notes
Board Meetings	Up to 20 years	Review and transfer to Place of Deposit	A local decision can be made on how long to retain the minutes of board meetings, and associated papers linked to the board meeting, but this must not exceed 20 years, and will be required to be transferred to the local PoD or The National Archives for National Bodies
Board Meetings (Closed Boards)	Up to 20 years	Review and Transfer to a Place of Deposit	Although these may still contain confidential or sensitive material, they are still a public record and must be transferred at 20 years, and any FOI exemptions noted, or indications that the duty of confidentiality applies.
Chief Executive records	Up to 20 years	Transfer to a Place of Deposit	This may include emails and correspondence where they are not already included in the board papers.
Committees: (major) - listed in the Scheme of delegation or that report into the Board (including major projects)	Up to 20 years	Transfer to a Place of Deposit	
Committees (minor) not listed in the scheme of delegation	6 years	Review and consider transfer to Place of Deposit	Includes minor meetings, projects, and departmental business meetings. These may have local historical value and require transfer consideration.

Data Protection Impact Assessments (DPIA's)	6 years	Review and destroy if no longer required	Should be kept for the life of the activity to which it relates, plus six years after that activity ends. If the DPIA was one-off, then 6 years from completion.
Destruction Certificates or record of information held on destroyed physical media	20 years	Review and dispose of if no longer required	Where a record is listed for potential transfer to PoD have been destroyed without adequate appraisal, consideration should be given to a selection of these as an indicator of what has not been preserved.
Incidents (serious)	20 years	Review and consider transfer to a Place of Deposit	Retention begins from the date of the Incident; not when the incident was reported.
Incidents (not serious)	10 years	Review and if no longer needed destroy	Retention begins from the date of the incident; not when the incident was reported.
Incidents (serious incidents requiring investigation)	20 years	Review and consider transfer to PoD	These include independent investigations into incidents. These may have permanent retention value so consult with the local PoD. If they are not required, then destroy.

Non-Clinical Quality Assurance Records	12 years	Review and if no longer needed destroy	Retention begins from the end of the year to which the assurance relates.
Patient Advice and Liaison Service (PALS) records	10 years	Review and if no longer needed destroy	Retention begins from the close of the financial year to which the record relates.
Patient surveys – individual returns and analysis	1 year after return	Review and destroy if no longer required	May be required again if analysis is reviewed.
Patient surveys – final report	10 years	Review and consider transfer to Place of Deposit	Organisations may want to keep final reports for longer than the raw data and analysis, for trend analysis over time. This period can be extended, provided there is justification and organisational approval.
Policies, strategies and operating procedures including business plans	Life of organisation plus 6 years	Review and consider transfer to a Place of Deposit	Retention begins from when the document is approved, until superseded. If the retention period reaches 20 years from the date of approval, then consider transfer to PoD
Quarterly reviews from NHS trusts	6 years	Review and destroy if no longer required	Retention period in accordance with the Limitation Act 1980.

Risk Registers	6 years	Review and destroy if no longer required	Retention period in accordance with the Limitation Act and corporate awareness of risks.
Staff surveys – individual returns and analysis	1 year after return	Review and destroy if no longer required	Forms are anonymous so do not contain PID unless provided in free text boxes. May be required again if analysis is reviewed.
Staff surveys – final report	10 years	Review and consider transfer to PoD	Organisations may want to keep final reports for longer than the raw data and analysis, for trend analysis over time. This period can be extended, provided there is justification and organisational approval.
Trust Submission Forms	6 years	Review and destroy if no longer required	Retention period in accordance with the Limitation Act 1980.

7.Communications			
Record Type	**Retention period**	**Action at end of retention period**	**Notes**
Intranet site	6 years	Review and consider transfer to a Place of Deposit	
Patient information leaflets	6 years	Review and consider transfer to a Place of Deposit	These do not need to be leaflets from every part of the organisation. A central copy can be kept for potential transfer.
Press releases and important internal communications	6 years	Review and consider transfer to a Place of Deposit	Press releases may form a significant part of the public record of an organisation which may need to be retained.
Public consultations	5 years	Review and consider transfer to a Place of Deposit	Whilst these have a shorter retention period, there may be wider public interest in the outcome of the consultation (particularly where this resulted in changes to the services provided) and so may have historical value
Website	6 years	Review and consider transfer to a Place of Deposit	The PoD may be able to receive these by a regular crawl. Consult with the PoD on how to manage the process. Websites are complex objects, but crawls can be made more effective if certain steps are taken: http://www.nationalarchives.gov.uk/webarchive/guidance/

8.Staff Records & Occupational Health

Record Type	Retention period	Action at end of retention period	Notes
Duty Roster	6 years	Review and if no longer needed destroy	Retention begins from the close of the financial year.
Exposure Monitoring information	40 years or 5 years from the date of the last entry made in it	Review and if no longer needed destroy	A) Where the record is representative of the personal exposures of identifiable employees, for at least 40 years or B) In any othercase, for at least 5 years.
Occupational Health Reports	Keep until 75th birthday or 6 years after the staff member leaves whichever is sooner	Review and if no longer needed destroy	

Occupational Health Report of Staff member under health surveillance	Keep until 75th birthday	Review and if no longer needed destroy	
Occupational Health Report of Staff member under health surveillance where they have been subject to radiation doses	50 years from the date of the last entry or until 75th birthday, whichever is longer	Review and if no longer needed destroy	
Staff Record	Keep until 75th. birthday (see Notes)	Review, and consider transfer to Place of Deposit	This includes (but is not limited to) evidence of right to work, security checks and recruitment documentation for the successful candidate including job adverts and application forms. Some PoDs accession NHS staff records for social history purposes. Check with your local PoD about possible accession. If the PoD does not accession them, then the records can be securely destroyed once the retention period has been reached.
Staff Record Summary	75th Birthday	Place of Deposit should be offered for continued retention or destroy	Some organisations create summaries after a period of time since the staff member left (usually 6 years). This practice is OK to continue if this is what currently occurs. The summary, however, needs to be kept until the staff member's 75th birthday, and then consider transferring to PoD. If the PoD does not require them, then they can be securely destroyed at this point.

Timesheets (original record)	2 years	Review and if no longer needed destroy	Retention begins from creation.
Staff Training records	See Notes	Review and consider transfer to a Place of Deposit	Records of significant training must be kept until 75th birthday or 6 years after the staff member leaves. It can be difficult to categorise staff training records as significant as this can depend upon the staff member's role. The following is recommended: • **Clinical training records** - to be retained until 75th birthday or six years after the staff member leaves, whichever is the longer. • **Statutory and mandatory training records** - to be kept for ten years after training is completed. • **Other training records -** keep for six years after training completed.
Disciplinary Records	6 years	Review and if no longer needed destroy	Retention begins once the case is heard, and any appeal process is completed. The record may be retained for longer, but this will be a local decision based on the facts of the case. The more serious the case, the more likely it will attract a longer retention period. Likewise, a one-off incident may need to only be kept for the minimum time stated. This applies to all cases, regardless of format.

9.Procurement

Record Type	Retention period	Action at end of retention period	Notes
Contracts sealed or unsealed	Retain for 6 years after the end of the contract	Review and if no longer needed destroy	
Contracts - financial approval files	Retain for 15 years after the end of the contract	Review and if no longer needed destroy	
Contracts - financial approved suppliers' documentation	Retain for 11 years after the end of the contract	Review and if no longer needed destroy	
Tenders (successful)	Retain for 6 years after the end of the contract	Review and if no longer needed destroy	
Tenders (unsuccessful)	Retain for 6 years after the end of the contract	Review and if no longer needed destroy	

10.Estates			
Record Type	**Retention period**	**Action at end of retention period**	**Notes**
Building plans Including records of major building work	Lifetime of the building or disposal of asset plus 6 years	Review and consider transfer to a Place of Deposit	Building plans and records of works are potentiallyof historical interest and where possible be kept and transferred to a place of deposit
CCTV (Closed circuit television)	See ICO Code of Practice	Review and if no longer needed destroy	The length of retention must be determined by the purpose for which the CCTV has been used. CCTV footage must remain viewable for the length of time it is retained, and where possible, systems should have redaction or censoring functionality to be able to blank out the faces of people who are captured by the CCTV, but not subject to the access request, for example, police reviewing CCTV as part of an investigation.
Equipment monitoring and testing and maintenance work where asbestos is a factor	40 years	Review and if no longer needed destroy	Retention begins from the completion of the monitoring or testing. This includes records of air monitoring and health records relating to asbestos exposure, as required by the Control of Asbestos Regulations 2012. https://www.legislation.gov.uk/uksi/2012/632/contents/made
Equipment monitoring – general testing and maintenance work	Lifetime of installation	Review and if no longer needed destroy	Retention begins from the completion of the testing and maintenance.
Inspection reports	Lifetime of installation	Review and if no longer needed destroy	Retention begins at the END of the installation period. Building inspection records need to comply with the Construction (Design and Management) Regulations 2015.

Leases	12 years	Review and if no longer needed destroy	Retention begins at point of lease termination.
Minor building works	6 years	Review and if no longer needed destroy	Retention begins at the point of WORKS COMPLETION
Photographic collections - service locations and events and activities	Up to 20 years	Review and consider transfer to Place of Deposit	These provide a visual historical legacy of the running and operation of an organisation. They may also provide secondary uses, such as use in public inquiry
Surveys: building or installation, not patient surveys	Lifetime of installation or building	Review and consider transfer to Place of Deposit	Retention period begins at the END of INSTALLATION period. See Inspection reports for legal basis for these records.

11.Finance

Record Type	Retention period	Action at end of retention period	Notes
Accounts	3 years	Review and if no longer needed destroy	Retention begins at the CLOSE of the financial year to which they relate. Includes all associated documentation and records for the purpose of audit.
Benefactions	8 years	Review and consider transfer to Place of Deposit	These may already be in the financial accounts and may be captured in other reports, records or committee papers. Benefactions, endowments, trust fund or legacies should be offered to the local PoD.
Debtor records - cleared	2 years	Review and if no longer needed destroy	Retention begins at the CLOSE of the financial year to which they relate
Debtor records - not cleared	6 years	Review and if no longer needed destroy	Retention begins at the CLOSE of the financial year to which they relate
Donations	6 years	Review and if no longer needed destroy	Retention begins at the CLOSE of the financial year to which they relate
Expenses	6 years	Review and if no longer needed destroy	Retention begins at the CLOSE of the financial year to which they relate
Final annual accounts report	Up to 20 years	Review and transfer to place of deposit	These should be transferred when practically possible, after being retained locally for a minimum of 6 years. Ideally, these will be transferred with board papers for that year to keep a complete set of governance papers

Financial transaction records	6 years	Review and if no longer needed destroy	Retention begins at the CLOSE of the financial year to which they relate.
Invoices	6 years from end of the financial year they relate to	Review and destroy if no longer required	Retention begins at the CLOSE of the financial year to which they relate.
Petty cash	2 years	Review and if no longer needed destroy	Retention begins at the CLOSE of the financial year to which they relate.
Private Finance initiative (PFI) files	Lifetime of PFI	Review and consider transfer to Place of Deposit	Retention begins at the END of the PFI agreement. This applies to the key papers only in the PFI.
Staff Salary information or files	10 years	Review and if no longer needed destroy	Retention begins at the CLOSE of the financial year to which they relate.
Superannuation records	10 years	Review and if no longer needed destroy	Retention begins at the CLOSE of the financial year to which they relate.

12.Legal, Complaints & Information Rights

Record Type	Retention period	Action at end of retention period	Notes
Complaints case file	10 years	Review and if no longer needed destroy	Retention begins at the CLOSURE of the complaint. The complaint is not closed until all processes (including potential and actual litigation) have ended. The detailed complaint file must be kept separately from the patient file (if the complaint is raised by a patient or in relation to). Complaints files must always be separate.
Fraud case files	6 years	Review and if no longer needed destroy	Retention begins at the CLOSURE of the case. This also includes cases that are both proven and unproven.
Freedom of Information (FOI) requests and responses and any associated correspondence	3 years	Review and if no longer needed destroy	Retention begins from the CLOSURE of the FOI request. Where redactions have been made, it is important to keep a copy of the response and send to the requestor. In all cases, a log must be kept of requests and the response sent.
FOI requests where there has been a subsequent appeal	6 years	Review and if no longer needed destroy	Retention begins from the CLOSURE of the appeal process.
Industrial relations including tribunal case records	10 years	Review and consider transfer to a Place of Deposit	Retention begins at the CLOSE of the financial year to which it relates. Some organisations may record these as part of the staff record, but in most cases, they should form a distinctive separate record (like complaints files).
Litigation records	10 years	Review and consider transfer to a Place of Deposit	Retention begins at the CLOSURE of the case. Litigation cases of significant or major issues (or with significant, major outcomes) should be considered for transfer. Minor cases should not be considered for transfer. If in doubt, consult with the PoD.

Intel Patents / trademarks / copyright / intellectual property	Lifetime of patent or 6 years from end of licence/ action	Review and consider transfer to Place of Deposit	Retention begins at the END of lifetime or patent, or TERMINATION of licence or action.
Software licences	Lifetime of software	Review and if no longer needed destroy	Retention begins at the END of lifetime of software.
Subject Access Requests (SAR), response, and subsequent correspondence	3 years	Review and if no longer needed destroy	Retention begins at the CLOSURE of the SAR.
Subject Access Request (SAR) where there has been an appeal	6 years	Review and if no longer needed destroy	Retention begins at CLOSURE of appeal.