Alder Hey Children's NHS
NHS Foundation Trust

Reference Number: FOI202223//595
From: Private Individual

Date: 16 February 2023

Subject: Protocols and procedures storage of records and retention dates

Q1 Can I request the protocols and procedures on how you store records and the retention dates please

A1 Please see attached for the following documents:

- Corporate Record Management Policy - RM38 DMS_Redacted
- Records Management Policy - RM38 (Archived on DMS)_Redacted. Please note, this policy has been replaced by the Corporate Records Management Policy, so is not a current published policy.

Our Health Records Management Policy is currently under review.

Health Records are retained in line with the Records Management NHS Code of Practice which can be accessed via the following link: https://transform.england.nhs.uk/information-governance/guidance/records-management-code/

Staff names exempted under Section 40: Personal Information. Although the information relates to their public role and accountability for managing budgets, disclosure of names of all individuals may potentially have adverse consequences to the employees. Any names of staff that are available in the public domain are accessible via our website

- https://alderhey.nhs.uk/

Alder Hey Children's NHS Foundation Trust

RM38 – CORPORATE RECORD MANAGEMENT POLICY

Document Properties	
Version:	12
Name of Ratifying Committee:	Digital Oversight Committee (DOC)
Date Ratified:	07/11/2022
Name of Originator/Author:	[redacted], Information Governance Manager
Name of Approval Committee:	Operational IT Group
Date Approved:	14/09/2022
Executive Sponsor:	Kate Warriner, Chief Digital & Information Officer
Date Issued:	10/11/2022
Review Date:	13/07/2023

1. Version Control, Review and Amendment Logs

Version Control Table				
Version	**Date**	**Author**	**Status**	**Comment**
12	November 2022	[redacted]	Current	Formal review
Records Management Policy – M38				
11.1	September 2022	[redacted]	Archived	Extension
11	September 2021	Cyber Security Manager	Archived	Add specific reference to digital files
10	May 2020	Data Protection Officer	Archived	DPO review and update across whole Policy, incorporating previous updated versions
9	December 2019	Health Records Manager, IG Manager	Archived	Reviewed and redrafted
8	April 2019	IG Manager	Archived	Updated to reflect changes in legislation
7	January 2018	IG Manager Health Records Manager	Archived	Title edited: RM38 – Records Management Policy
6.1	July 2015	Health Records Manager, IG Manager	Archived	Addition of paragraph on record keeping audit
6	April 2015	Health Records Manager IG Manager	Archived	Reviewed and re-written
5	February 2011	Health Records Manager IG Manager	Archived	This policy has been updated to reflect new CBU structure and reporting.
4	September 2010	Health Records Manager Information Governance Co-ordinator	Archived	This policy has been changed to reflect the new reporting arrangements. The newly formed Records Management Steering Group will now monitor this policy rather than the Information Governance Steering Group.
3	February 2010	Health Records Manager IG Co-ordinator	Archived	Clinical and Corporate Records included
2	October 2006	Health Records Manager IG Co-ordinator	Archived	
1	March 2004	Unknown	Archived	

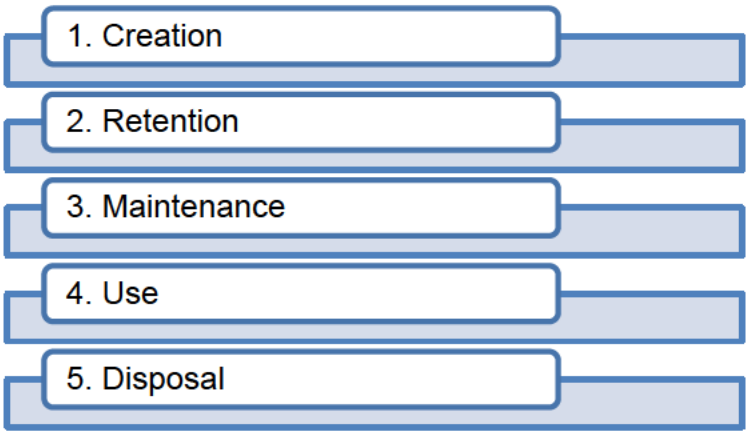
Record of changes made to Corporate Record Management Policy – RM38 – Version 12			
Section Number	**Page Number**	**Change/s made**	**Reason for change**
All sections	All pages	Policy title amended and complete re-write of content	IG collaborative working between Alder Hey and Liverpool Heart and Chest Hospital. Policy aligned with LHCH. New Health Records Management policy to be created.

2. Quick Reference Guide – Corporate Record Management Policy

This document sets out the Trust's management arrangements for corporate records. The Trust has developed appropriate processes and procedures for the management of records, including the secure destruction of records both physical and digital.

The policy aims to provide staff with advice and support during the lifecycle of any record created or used during the performance of our duties.

Record Lifecycle



The Trust has a statutory obligation to maintain accurate records of its activities and these records are public records under UK law.

Records are the Trust's 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 rights of patients, staff, and members of the public.

Records support consistency, continuity, efficiency, productivity and help deliver services in consistent and equitable ways.

Contents

3. Introduction

Alder Hey Children's Hospital (hereafter called the Trust) is committed to ensuring that there is an organisation-wide policy, with clear lines of accountability to the Trust Board, for the management of corporate records.

Records management is the process by which the Trust manages all aspects of records whether internally or externally generated and in any format or media type, from their creation, all the way through to their lifecycle to their eventual disposal. The Trust has a statutory obligation to maintain accurate corporate records of its activities and these records are public records under the terms of the Public Records Acts 1958 and 1967.

Records are a valuable resource because of the information they contain. Information is only usable if it is correctly recorded, is regularly updated and is easily accessible when needed.

Records are the Trust's 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.

Purpose

The purpose of this policy is to:

- outline how the Trust's corporate records will be managed and controlled
- ensure that corporate records are managed and controlled effectively
- meet legal, operational, and organisational information requirements
- ensure records are readily accessible and available for use
- eventually archived or disposed efficiently and effectively

Scope

This policy applies to:

- All employees of the Trust, both permanent and temporary
- Anyone contracted to the Trust, who in the course of their work is required to create and/or access corporate records normally restricted to directly employed staff
- All corporate records held in all formats, see Appendix A for examples of formats and types

This policy **does not** apply to clinical / patient health records.

4. Definitions

APPRAISAL
The process of evaluating an organisation's activities to determine which records should be kept, and for how long, to meet the needs of the organisation, the requirements of Government accountability and the expectations of researchers and other users of the records. (The National Archives, Records Management Standard RMS 1.1)

The process of distinguishing records of continuing value from those of no value so that the latter may be eliminated. (The National Archives, Definitions in the Context of the Seamless Flow Programme)

AUTHENTICITY
An authentic record is one that can be proven:

- to be what it purports to be;
- to have been created or sent by the person purported to have created or sent it; and
- to have been created or sent at the time purported.

CLASSIFICATION
The systematic identification and arrangement of business activities and/or records into categories according to logically structured conventions, methods and procedural rules represented in a classification system. (BS ISO 15489-1:2001(E))

CORPORATE RECORDS
Records (other than health records) that are of, or relating to, an organisation's business activities covering all the functions, processes, activities and transactions of the organisation and of its employees. Including documents that contain information which supports a decision-making process of any description. See Appendix A for examples of formats and types

CURRENT RECORDS
Records necessary for conducting the current and ongoing business of an organisation.

DESTRUCTION
The process of eliminating or deleting records beyond any possible reconstruction. (BS ISO 15489-1.2001(E))

DISPOSAL
Disposal is the implementation of appraisal and review decisions. These comprise the destruction of records and the transfer of custody of records (including the transfer of selected records to an archive institution). They may also include the movement of records from one system to another (for example, paper to electronic). (The National Archives, Records Management Standard RMS1.1)

ELECTRONIC RECORD MANAGEMENT SYSTEM
A system that manages electronic records throughout their lifecycle, from creation and capture through to their disposal or permanent retention, and which retains their integrity and authenticity while ensuring that they remain accessible. (The National Archives, Definitions in the Context of the Seamless Flow Programme)

FILE
An organised unit of documents grouped together either for current use by the creator or in the process of archival arrangement, because they relate to the same subject, activity or transaction. A file is usually the basic unit within a records series.

FILING SYSTEM
A plan for organising records so that they can be found when needed. (The National Archives, Records Management Standard RMS 1.1)

INDEXING
The process of establishing access points to facilitate retrieval of records and/or information. (BS ISO 15489-1:2001(E))

INFORMATION AUDIT
An information audit looks at the means by which an information survey will be carried out and what the survey is intended to capture.

INFORMATION COMMISSIONER
The Information Commissioner enforces and oversees the Data Protection Act 1998 and the Freedom of Information Act 2000.

INFORMATION SURVEY/RECORDS AUDIT
A comprehensive gathering of information about records created or processed by an organisation. (The National Archives, Records Management Standards and Guidance – Introduction Standards for the Management of Government Records)

It helps an organisation to promote control over its records and provides valuable data for developing records appraisal and disposal procedures. It will also help to:

- identify where and when health and other records are generated and stored within the organisation and how they are ultimately archived and/or disposed of and
- accurately chart the current situation in respect of records storage and retention organisation-wide, to make recommendations on the way forward and the resource implications to meet existing and future demands of the records management function.

INTEGRITY OF RECORDS
The integrity of a record refers to its being complete and unaltered. It is necessary that a record be protected against unauthorised alteration. Records management policies and procedures should specify what additions or annotations may be made to a record after it is created, under what circumstances additions or annotations may be authorised and who is authorised to make them. Any unauthorised annotation, addition or deletion to a record should be explicitly identifiable and traceable.

MICROFORM
Records in the form of microfilm or microfiche, including aperture cards.

MIGRATION (see also CONVERSION)
The act of moving records from one system to another, while maintaining the records' authenticity, integrity, reliability, and usability. (BS ISO 15489-1:2001(E))

MINUTES (MASTER COPIES)
Master copies are the copies held by the secretariat of the meeting, ie the person or department who actually takes, writes and issues the minutes.

MINUTES (REFERENCE COPIES)
Copies of minutes held by individual attendees at a given meeting.

NHS RECORDS (Public Records Act)
All NHS records are public records under the terms of the Public Records Act 1958 sections 3(1) – (2). All records created and used by NHS employees are public records.

PAPER RECORDS
Records in the form of files, volumes, folders, bundles, maps, plans, charts, etc.

PERMANENT RETENTION
Records may not ordinarily be retained for more than 30 years. However, the Public Records Act provides for records which are still in current use to be legally retained. Additionally, under separate legislation, records may need to be retained for longer than 30 years, for example Occupational Health Records relating to the COSSH

(Control of Substances Hazardous to Health) Regulations, or records required for variant CJD surveillance.

Section 33 of the Data Protection Act permits personal data identified as being of historical or statistical research value to be kept indefinitely as archives.

PROTECTIVE MARKING
The process of determining security and privacy restrictions on records.

PUBLICATION SCHEME
A publication scheme is required of all NHS organisations under the Freedom of Information Act. It details information which is available to the public now or will be in the future, where it can be obtained from and the format it is or will be available in. Schemes must be approved by the Information Commissioner and reviewed periodically to make sure they are accurate and up to date.

PUBLIC RECORDS
Records as defined in the Public Records Act 1958 or subsequently determined as public records by The National Archives.

Records of NHS organisations (and those of predecessor bodies to NHS organisations) are defined as public records under the terms of the Public Records Act 1958 sections 3(1)–(2). NHS records are not owned by the NHS organisation that created them and may not be retained for longer than 30 years without formal approval by The National Archives. (The National Archives)

Records of services supplied within NHS organisations but by outside contractors are not defined as public records but are subject to the Freedom of Information Act.

RECORDS
Information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations, or in the transaction of business. (BS ISO 15489.1)

An NHS record is anything which contains information (in any media) which has been created or gathered as a result of any aspect of the work of NHS employees – including consultants, agency or casual staff.

RECORDS MANAGEMENT
Field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records. (BS ISO 15489-1:2001(E))

RECORD SERIES
A series is the main grouping of records with a common function or subject – formerly known as ‘class’. (The National Archives)

Documents arranged in accordance with a filing system or maintained as a unit because they result from the same accumulation or filing process, or the same activity,

because they have a particular form, or because of some other relationship arising out of their creation, receipt, or use. (International Council on Archives' (ICA) General International Standard Archival Description or ISAD(G)) – http://www.icacds.org.uk/eng/ISAD(G).pdf

A series comprises the record of all the activities that are instances of a single process. A series may be large or small: it is distinguished not by its size, but by the fact that it provides evidence of a particular process. If an activity takes place that is unique, rather than an instance of a process, its records form a series in their own right. (Elizabeth Shepherd and Geoffrey Yeo, Managing Records: a handbook of principles and practice (Facet 2003))

RECORD SYSTEM/RECORD-KEEPING SYSTEM
An information system which captures manages and provides access to records through time. (The National Archives, Records Management: Standards and Guidance – Introduction Standards for the Management of Government Records)

Records created by the organisation should be arranged in a record-keeping system that will enable the organisation to obtain the maximum benefit from the quick and easy retrieval of information. Record-keeping systems should contain descriptive and technical documentation to enable the system and the records to be understood and to be operated efficiently, and to provide an administrative context for effective management of the records, including a documented set of rules for referencing, titling, indexing and, if appropriate, the protective marking of records. These should be easily understood to enable the efficient retrieval of information and to maintain security and confidentiality.

REDACTION
The process of removing, withholding or hiding parts of a record due to either the application of a Freedom of Information Act exemption or a decision by The National Archives to restrict access where sensitivity, copyright or data protection issues arise. (The National Archives, Definitions in the Context of the Seamless Flow Programme)

REGISTRATION
Registration is the act of giving a record a unique identifier on its entry into a record-keeping system.

RETENTION
The continued storage and maintenance of records for as long as they are required by the creating or holding organisation until their eventual disposal, according to their administrative, legal, financial, and historical evaluation.

REVIEW
The examination of records to determine whether they should be destroyed, retained for a further period, transferred to an archival establishment, or presented to a third party (for example a university).

TRACKING
Creating, capturing and maintaining information about the movement and use of records. (BS ISO 15489-1:2001(E))

TRANSFER OF RECORDS
Transfer (custody) – Change of custody, ownership and/or responsibility for records. (BS ISO 15489-1:2001(E))

Transfer (movement) – Moving records from one location to another. (BS ISO 15489-1:2001(E))

Records identified as more appropriately held as archives should be offered to The National Archives, which will make a decision regarding their long-term preservation.

VERSION CONTROL
Is the management of multiple revisions to the same document and differentiates one version of a document from another. Version control is important:

- for documents that undergo a lot of revision and redrafting and is particularly important for electronic documents because they can easily be changed by several different users, and those changes may not be immediately apparent.
- when working on a collaborative document with several contributors and/or frequent revisions, for example a consultation response

VERSION NUMBERS
A simple version control technique where a unique version number is applied to a document to distinguish one version from another. This procedure should be used for all documents where more than one version exists or is likely to exist in the future.

A version numbering system that uses version numbers with points to reflect major and minor changes can be used, such as version 1.1 (first version with minor change), version 2.0 (second version with a major change), version 2.1 (third version with a minor change). The version number and date on the document itself.

WEEDING
The process of removing inactive/non-current health records from the active/current or primary records storage area to a designated secondary storage area after a locally agreed timescale after the date of last entry in the record.

5. Duties

The **Chief Executive** is the Trust's accountable officer for records management. Senior managers are responsible for the quality of the records management within their respective departments and all line managers must ensure that their staff are appropriately trained and apply the associated guidelines and procedures.

The **Chief Digital and Information Officer** is responsible for the implementation of the contents of this policy in line with the action plans approved by the Risk Management & Corporate Governance Committee.

The **Senior Information Risk Officer (SIRO)** is responsible for approving and ensuring that national and local guidelines and protocols on the handling and management of confidential corporate information and person identifiable information (non-patient) are in place.

The **Caldicott Guardian** is responsible for approving and ensuring that national and local guidelines and protocols on the handling and management of confidential patient information are in place.

The **Head of IG and Data Protection Officer** provides independent advice on the Trust's data processing activities and will support the development of policies, procedures, and other measures to ensure data protection compliance.

The **Information Governance Manager** will ensure that the policies and procedures associated with this policy are maintained and promoted around the Trust.

Divisional Heads of Operation / Heads of Service are responsible for local records management within their service and the development of procedures to ensure that records are controlled and managed in line with this policy.

All **line managers and supervisors** are responsible for ensuring that their staff are made aware of and adhere to this policy: are adequately trained; and apply the appropriate guidelines when handling corporate records.

All **Alder Hey Children's Hospital staff** are responsible for co-operating with the development and implementation of corporate policies as part of their normal duties and responsibilities.

Temporary or agency staff, contractors, students or others will be expected to comply with the requirements of all Trust policies applicable to their area of operation.

6. Controlled document standards

Data Protection Act 2018 / General Data Protection Regulation - regulates the processing of personal data, held manually and on computer.

Freedom of Information Act 2000 - requires public bodies including the NHS to keep and make information available on request.

Public Records Act 1958 - requires that records selected for archival preservation are transferred to the National Archives or a 'Place of Deposit' appointed under the Act.

Records Management Code of Practice for Health and Social Care 2016 – provides guidance on management and use of records and the minimum retention periods.

Government Security Classification Scheme (GSCS) – sets out how central government and public sector organisations classify information to ensure it is appropriately protected.

Section 45 Code of Practice – sets out the practices with public authorities should follow when dealing with requests for information under the Freedom of Information Act

Section 46 Code of Practice – provides guidance on good practice in records management for public bodies subject to the Freedom of Information Act

7. Procedure

3.1 Principles of corporate records management

Records are valuable because of the information they contain. Good record keeping must ensure that:

- NHS employees can work with maximum efficiency
- there is an audit trial which enables any record entry to be traced to a named individual with the knowledge that all alterations can be similarly traced
- any decisions made can be justified or reconsidered at a later date

Records must be:

- Correct
- Legibly recorded
- Kept up to date
- Easily accessible
- Kept for a minimum retention period

All employees must ensure that corporate records are:

- relevant and complete: important information must be recorded
- held in an appropriate format
- legible, where held manually
- kept in directorate folders were held electronically
- up to date
- disposed of when no longer required, either through archiving or through waste disposal, in line with the retention policy

Key components of records management

- record creation
- record keeping
- record maintenance (including tracking of record movements)
- access and disclosure
- closure and transfer
- review
- archiving
- disposal

3.2 Creation

Records of operational and business activities must be complete and accurate and staff should ensure that they formally record all decisions and transactions made in the course of their official business, for example making file notes of telephone conversations and minutes of meetings etc.

Records must be placed into an indexed and organised filing structure; this includes all official communications, including letters, faxes and emails.

Each department and service must create an inventory of the corporate records held and develop local standard operating procedures covering record creation, including naming, referencing, classification and filing structure for both paper and electronic records.

The agreed filing structure should be clear and logical to aid retrieval of records and help with the management of the retention and disposal of records.

All electronic records must be held in folders on the Trust's networked shared drives ensuring routine back-up of data. Records must not be saved to local or personal drives on PCs or to any portable media. Only those people who need to have access to the folders should have access.

Paper records must be kept in designated filing cabinets and cupboards and must normally be kept locked to prevent unauthorised access.

Each department and service is responsible for ensuring that a system is established so that drawers containing corporate records are kept locked when not in use, and with a key holder and deputy key holder system in place.

3.3 Referencing/Naming

Departments and services should use a referencing system that meets their operational business needs and which can be easily understood by staff that create documents and records, for example alphanumeric; alphabetical; numeric; keyword.

Referencing information should be detailed within the footer section of electronic documents as follows:

- Author
- Date created
- File reference
- Version number
    - Draft documents should be clearly marked 'draft' until finalised. Draft documents should be numbered as follows – first draft 0.1; second draft 0.2 etc. until the document is finalised
    - Documents should be numbered as follows - first document 1.0; second document 2.0 etc. Minor changes to the document may however be evidenced by decimal numbers e.g. 2.1
    - Finalised documents should be protected to prevent changes being made to the original document, e.g. conversion to PDF format.

A document becomes a record when it has been finalised and becomes part of the Trust's corporate information. At this point, the record must not be amended and should only be held in the corporate system, for example, the network shared drive and not on a local drive on a personal computer or laptop.

Documents which have not been finalised still belong to the Trust and are still

information held for the purposes of Freedom of Information Act 2000 (FOIA) and may still be placed into the public domain.

Paper records must be kept securely but accessible to those who require access. The following factors must be considered:

- compliance with health and safety regulations
- degree of security required
- users' needs
- type of record to be stored
- size and quantity of record
- usage and frequency of retrievals
- space, efficiency, and price

A paper document becomes a record when it has been finalised and become part of the Trust's corporate information. At this point, the record must not be amended and must only be held in the corporate filing system and not in a personal desk drawer.

3.4 Classification

In line with the Trust's Information Security Management System (ISMS) policy all corporate records, whether they are held electronically or in paper format, must be classified in line with the Government Security Classification Scheme (GSCS).

Security classifications indicate the sensitivity of the information and provide a set of baseline security controls to provide an appropriate level of protection. See ISMS Security Standard 2 for details.

Please note that regard must be paid to the requirements of the Freedom of Information Act 2000 when classifying records. While classification marking of information can assist in assessing whether exemptions to the Freedom of Information Act 2000 may apply, each FOI requests must however be considered on its own merits and the classification in itself is not a justifiable reason for exemption.

The Information Governance Team can provide further guidance on exemptions – info.gov@alderhey.nhs.uk or 0151 600 1845.

3.5 Tracking and Tracing

The movement and location of physical records must be controlled and there should be tracking and tracing procedures in place that provide an auditable trail of the records.

Each department and service is responsible for local standard operating procedures to ensure that tracking systems are established so that any file or document which is removed from its usual place, is easily traceable to the person who currently holds it. This is of particular importance where the master corporate record is solely held in paper format.

3.6 Management of Email

The email system is a corporate business tool and email messages sent and received can constitute corporate records.

Emails relating to business activities are corporate records while routine email messages are not. For example, completed email exchanges about a transaction, decision or communication about an issue are business activities however an email confirming attendance at a meeting is routine and would not need to be saved for any length of time.

All members of staff are responsible for identifying and managing email messages appropriately. Appendix B provides guidance on email record management.

It is important that email messages and their attachments identified as business activity records are moved from personal or group mailboxes to be managed in the same way as other corporate records. Emails should be saved into a shared folder on the Trust's network, secured with the appropriate access permissions. Emails should be retained where there is a legal or operational requirement to do so in line with the Trust's Record Retention Schedule.

The email system does not provide unlimited email storage and should not be treated as a record or information archive therefore once an email message has been saved to the network it should be deleted from the email system.

Personal mailboxes should not be used for long-term storage of email messages. Personal mailboxes should be used for personal information or short-term reference purposes, when these emails are no longer required, they should be deleted.

Group mailboxes should not be used for long-term storage of email messages. Group mailboxes (inbox and temporary sub-folders) should be used for short-term business activities (work in progress) or short-term reference purposes. When the business activity has been completed the relevant email messages and attachments should be saved into the appropriate network folder. Short-term reference emails should be deleted when no longer required.

Emails like other corporate records are subject to record management legislation and staff must not delete emails if they know or suspect the message is or may become subject to a request for information under Freedom of Information or Data Protection legislation.

3.7 Retention and Disposal

Corporate records must be retained for the minimum period of time for legal, operational, research and safety reasons.

The length of time for retaining records will depend on the type of record and its importance to the Trust's business functions.

The Trust has adopted the retention periods set out in the Records Management Code of Practice for Health and Social Care 2021 and records must be retained in accordance with this retention and destruction schedule.

If a specific record type is not detailed within the retention schedule, contact Information Governance for guidance and authority to establish a local retention period – info.gov@alderhey.nhs.uk or 0151 600 1845.

Records should be closed (made inactive and transferred to secondary storage) as soon as they stop being actively used.

During the retention period records must continue to be protected, maintained, easily located and useable.

Records must be reviewed for destruction prior to the end of the relevant retention period and those identified for archival preservation should be referred to the Information Governance Team for approval.

Records approved for transfer must be transferred to an archival institution as soon as possible. A list of approved places of deposit can be found on The National Archives website. Records must however be transferred no later than 20-years from creation of the record, as required by the Public Records Act 1958 and the 20-year rule and records of local interest.

Records identified for destruction must be securely destroyed and a record of the destruction, showing the records' reference, description and date of destruction must be maintained.

Corporate records must not be destroyed at the end of their retention period if there is:

- **an on-going complaint where the record may provide evidence or audit trail of events**
- **a Freedom of Information Act request is received before the document has been destroyed**
- **a Data Protection Act request where a corporate document may contain personal data of the applicant**
- **a legal claim is anticipated or is on-going where the records may provide evidence or audit trail of events**

Each Department/Service must create local standard operating procedures covering record retention and disposal for both paper and electronic records in line with this policy and associated procedures.

3.7 Corporate Records Audit

The Trust will undertake an audit of corporate records every three years. The audit will cover paper and electronic records both current and closed/archived, and will establish the:

- types and format of records held

- retention periods
- record keeping systems in use

The audit will cover at a minimum the records detailed in CQC Outcome 21 (Records Management) Prompt 12:

- Estates
- Financial
- Information
- Information Management & Technology (IM&T)
- Human Resources
- Purchasing/Supplies
- Complaints

Any issues identified such as unsecured records, records being kept too long or destroyed too soon will be feedback to the relevant service with an action plan and remedial recommendations implemented.

The audit report will be presented to the Risk Management Committee who will review and monitor progress against the action plans.

3.8 Records Management Systems

Records must be maintained in a system that ensures they are properly stored and protected throughout their lifecycle. Particular attention must be paid when migrating electronic records across to new systems.

The Trust will ensure that before introducing new systems or processes consideration is given to technological advances to ensure that records will remain accessible and retrievable when required.

Records management systems should ensure:

- There are audit trails showing when records are created; accessed, modified and disposed of
- There is a logical structure to records to aid filing and retrieval, and archiving and destruction
- There are suitable storage areas throughout the records lifecycle i.e. secure and accessible
- That records are controlled and protected through a range of security measures
- That all movement of records is tracked
- Technological upgrades are supported ensuring records remain accessible & usable
- Cross-referencing between electronic and paper records

8. Policy implementation plan

Statements within the policy and the associated Trust Information Governance policies will be supported through the work of the Risk Management Committee.

The Board will be responsible for implementation of the policy.

The Information Governance Manager is responsible for ensuring that policy content is included within staff awareness and training sessions. Records management will be covered in mandatory training and induction sessions, and specific awareness sessions will be undertaken as and when appropriate in response to changes in the relevant legislation.

Managers are responsible for ensuring that all staff receive support and guidance to enable them to comply with the requirements of this policy and its associated procedures.

Awareness of this policy will be raised via the Information Governance pages on the intranet and in Trust's corporate communication messages.

Copies of the policy will be accessible on the Document Management System.

9. Monitoring

Compliance with the policy will be monitored annually by the Risk Management Committee through review of:

- Records Management incidents
- FOI request compliance
- Corporate records audit results
- CQC Outcome 21 compliance

Monitoring	Lead Responsible	Frequency	Responsible Committee
Data security and protection breaches / incidents	IG Manager	Monthly	Operational IT Group
DSPT self-assessment and MIAA audit	IG Manager	Annual	Operational IT Group
Corporate records audit	IG Manager	Annual	Operational IT Group
FOI compliance	IG Manager	Monthly	Operational IT Group
ICO complaints	IG Manager	Monthly	Operational IT Group

10. Further Information

10.1. References

- Data Protection Act 2018 / UK General Data Protection Regulation
- Freedom of Information 2000
- Section 45 (Lord Chancellor's Code of Practice on the discharge of public authorities' functions under Part I of the FOIA)
- Section 46 (Lord Chancellor's Code of Practice on the management of records)
- Environmental Information Regulations 2004

- Records Management Code of Practice for Health and Social Care 2021 - https://transform.england.nhs.uk/information-governance/guidance/records-management-code/
- Government Security Classification Scheme (GSCS) - https://www.gov.uk/government/publications/government-security-classifications
- Confidentiality NHS Code of Practice
- National Archives Standard and Guidance lines on:
    - Developing a policy on managing email
    - File creation
    - Tracking records
    - 20-year rule and records of local interest
    - Places of Deposit
- Royal United Hospital Bath NHS Trust, NHS West Cheshire CCG, Leeds CCG, Hull CCG – local policy

10.2. Consultation and endorsements

Name of endorser or Committee Chair	Role/Position of endorser or name of endorsing committee	Date
Kate Warriner, CDIO	Operational IT Group Member	September 2022
[redacted], Assistant CDIO - Service Delivery & Assurance	Operational IT Group Member	September 2022
[redacted], Head of IG & DPO	Operational IT Group Member	September 2022
[redacted], Cyber Manager	Operational IT Group Member	September 2022
[redacted], Associate Director – Data & Analytics	Operational IT Group Member	September 2022
[redacted], Head of Data	Operational IT Group Member	September 2022
[redacted], Head of Operational IT	Operational IT Group Member	September 2022
[redacted], Head of Clinical Imaging Systems / CSO	Operational IT Group Member	September 2022
[redacted], Associate Director – Operation IT	Chair of Operational IT Group	September 2022

11. Appendices

11.1. Appendix A – Examples of Corporate record types and format

Corporate record types include, but is not restricted to:

- Action Plans
- Audits
- Board Papers
- Commissioning documents
- Committee Minutes and agendas
- Complaints records
- Contracts and Service Level Agreements
- Diaries (non-clinical)
- Email - completed exchanges
- Financial records
- Incident reports
- Internal communications (including e-mail, and text messages)
- Policies, strategies, procedures, guidelines, and protocols
- Substantive contributions to the developments of policy or procedures, including factual evidence and interpretive material relating to changes in policy etc.
- Risk Registers
- Staff records, Human Resource records
- Line managers - please refer to HR Department for guidance on documents to be retained in local staff records
- Webpages (intranet / internet)
- Background material which supports decisions, opinions and advice documents which form a key part of any audit trail
- Versions of key publications (e.g. corporate plans, annual reports, statistical returns
- Measures taken to comply with legal and other obligation (e.g. Health and Safety at Work Act)

Corporate record formats include:

- photographs, slides and other images
- microform (i.e. microfiche/microfilm)
- audio and video tapes, cassettes and CD-ROMs/DVDs, CCTV etc.
- emails
- text messages (both outgoing and incoming)
- computerised records (databases, output and disks)
- paper records
- scanned records
- material intended for short-term or transitory use including notes and spare copies of documents
- any portable media containing information
- any material which holds information

11.2. Appendix B – Email record management

The main points to consider when managing email messages are:

Identifying business activity emails	When an email is sent or received a decision needs to be made about whether the email needs to be captured as a corporate record. For example, at the start of a project, an email may include the setting out of key points for staff to consider in setting up a new process, this could be classed as a corporate record and needs to be saved with other documentation relating to the new process.
Deciding whether to email message, the attachment or both should be kept as a corporate record	In most cases the attachment or attachments should be captured as a corporate record with the email message because the message will provide the context within which the attachment was used. A copy of attachments requiring further work should be saved to another network location to be worked on.
Who is responsible for capturing email corporate records?	The lead for a particular business activity (project or specific piece of work) should routinely be responsible for capturing and keeping full email exchanges (messages and relevant attachments) relating to it. For example, the IG Team are responsible for capturing all email correspondence relating to FOI requests for information
When to capture email corporate records	Email messages and attachments identified as corporate records should be capture as soon as possible. Email conversation strings should be captured as records either at the end of the email exchange or at significant points during the conversation especially as it might not always be apparent when the exchange/conversation has finished.
Where to capture email records	Work in progress email messages such as ongoing exchanges/conversations should be saved into a temporary sub-folder of the email Inbox. The subfolder should be appropriately named. Completed business activity email messages should be saved into a shared folder on the Trust's network, secured with the appropriate access permissions alongside other records relating to the same business activity.

	For example, email messages and attachments relating to completed FOI requests are saved into the network folder for the respective FOI request.
Titling email corporate records	The subject line of email should give clear indication of the content of the message and be reflect the business activity to which it relates. The subject line will become the filename when saved to the network. Network folders containing corporate records should be clearly named to reflect the business activity it relates to.

11.3. Appendix C – Archive and destruction process

Retention period starts
↓
Index records for archiving using the **Contents List Template** or print out the record index
↓
Store locally or contact **Health Records** Paper.light@alderhey.nhs.uk to arrange offsite storage
↓
Retention period ends
↓
List records for destruction using the **Destruction template** attaching record index/contents list
↓
Review and approve listed records for destruction
↓
Securely destroy records

<table>
<tr><td colspan="4">↓</td></tr>
<tr><td>Paper records
Trust held</td><td>Paper records
held offsite</td><td>Electronic records
Trust held</td><td>Electronic records
3rd party held</td></tr>
<tr><td>↓</td><td>↓</td><td>↓</td><td>↓</td></tr>
<tr><td>Place into confidential waste bin</td><td>Instruct Health Records
Paper.light@alderhey.nhs.uk
to arrange destruction</td><td>Delete Files and/or folders</td><td>Instruct 3rd party supplier to delete and request confirmation</td></tr>
<tr><td colspan="4">↓</td></tr>
<tr><td colspan="4">Update Destruction Template with the date of destruction</td></tr>
<tr><td colspan="4">[the date placed into confidential waste; date files / folders were deleted; destruction date from the offsite certificate of destruction; destruction date confirmed by 3rd party]</td></tr>
<tr><td colspan="4">↓</td></tr>
<tr><td colspan="4">Forward completed Destruction Template to Information Governance info.gov@alderhey.nhs.uk</td></tr>
</table>

12. Checklist for Approval of Policies

		Yes/No/ Unsure	Comments
1.	**Title**		
	Is the title clear and unambiguous?	Yes	
	Is it clear that the document is a Trust policy?	Yes	
2.	**Rationale**		
	Are reasons for development of the policy stated?	Yes	Existing policy
3.	**Development Process**		
	Is the method described in brief?	N/A	Review of existing policy
	Are individuals involved in the development identified?	Yes	Circulated to members of the Trust's Operational IT Group for consultation
	Do you feel a reasonable attempt has been made to ensure relevant expertise has been used?	Yes	As above
	Is there evidence of consultation with stakeholders and users?	Yes	
4.	**Content**		
	Is the objective of the document clear?	Yes	
	Is the target population clear and unambiguous?	Yes	
	Are the intended outcomes described?	Yes	
	Are the statements clear and unambiguous?	Yes	
5.	**Evidence Base**		
	Is the type of evidence to support the document identified explicitly?	Yes	
	Are key references cited?	Yes	
	Are the references cited in full?	Yes	
	Are local/organisational supporting documents referenced?	Yes	
6.	**Approval**		
	Does the document identify which committee/group will approve it?	Yes	
	If appropriate, have the joint Human Resources/staff side committee (or equivalent) approved the document?	N/A	
7.	**Dissemination and Implementation**		
	Is there an outline/plan to identify how this will be done?	Yes	
	Does the plan include the necessary training/support to ensure compliance?	Yes	
8.	**Document Control**		
	Does the document include version history and identify key changes since the last approved version?	Yes	
9.	**Process for Monitoring Compliance**		

		Yes/No/ Unsure	Comments
	Are there measurable standards or KPIs to support monitoring compliance of the document?	Yes	
	Is there a plan to review or audit compliance with the document?	Yes	
10.	**Review Date**		
	Is the review date identified?	Yes	
	Is the frequency of review identified? If so, is it acceptable (Default is 3 years)?	Yes	
11.	**Overall Responsibility for the Document**		
	Is it clear who will be responsible for coordinating the dissemination, implementation and review of the documentation?	Yes	

The policy author is responsible for completing the above checklist prior to submission for approval.

13. Equality Impact Assessment

Initial Equality Impact Assessment (EIA) Form	
This section must be completed at the development stage i.e. before approval or ratification. For further guidance please refer to the Equality Impact Assessment (EIA) Policy on DMS.	
Part 1	
Name and Job Title of Responsible Person(s): [redacted], IG Manager and [redacted], Head of IG & DPO	**Contact Number:** 0151 600 1240
Department(s): Trust wide policy	**Date of Assessment**: 24/08/2022
Name of the policy / procedure being assessed: Corporate Record Management policy	
Is the policy new or existing? New ☐ Existing ☑	
Who will be affected by the policy (*please tick all that apply*)? Staff ☑ Patients ☑ Visitors ☑ Public ☑ - all individuals whose personal data is processed by the Trust (the data subjects)	
How will these groups / key stakeholders be consulted with? No direct consultation, policy summaries the Trust's approach to managing data in line with legal requirements set out in UK law.	
What is the main purpose of the policy? This policy outlines how the Trust will manage its corporate records …. The policy does not discriminate against any of the protected characteristics or groups.	
What are the benefits of the policy and how will these be measured? As above, the policy will ensure legal compliance and promote openness and transparency.	
Is the policy associated with any other policies, procedures, guidelines, projects or services? Yes ☑ No ☐ *If yes, please give brief details:* Code of Conduct for Handling Personal Data, Data Protection policy, Data security and protection breaches / Incident reporting policy, Safe haven policy, Information Risk policy, Corporate Information Disclosure policy, Overarching IT policy, Access to Health Records policy	
What is the potential for discrimination or disproportionate treatment of any of the protected characteristics? *Please use the **Equality Relevance** guidance (see on DMS) to specify who would be affected (e.g. patients with a hearing impairment, staff aged over 50).*	

Please tick either positive, negative or no impact then explain in reasons and include any mitigation e.g. requiring applicants to apply for jobs online would be negative as there is potential disadvantage to individuals with learning difficulties or older people (detail this in the reason column with evidence) however applicants can ask for an offline application as an alternative (detail this in the mitigation column)

Protected Characteristic	**Tick either positive, negative or no impact**			**Reasons to support your decision and evidence sought**	**Mitigation / adjustments already put in place**
	Positive Impact *(benefit)*	**Negative *(disadvantage or potential disadvantage)***	**No Impact**		
Age	☐	☐	☑		
Sex	☐	☐	☑		
Race	☐	☐	☑		
Religion or belief	☐	☐	☑		
Disability	☐	☐	☑		
Sexual orientation	☐	☐	☑		
Pregnancy and maternity	☐	☐	☑		
Gender reassignment	☐	☐	☑		
Marriage and civil partnership	☐	☐	☑		
Other (specify)	☐	☐	☑		

If you have identified no negative impact for all please explain how you reached that decision and provide reference to any evidence (e.g. reviews undertaken, surveys, feedback, patient data etc.)
Click or tap here to enter text.

Does the policy raise any issues in relation to Human Rights as set out in the Human Rights Act 1998? Yes ☐ No ☑
*See **Equality Relevance** guidance (on DMS) for more details (NB if an absolute right is removed or affected the policy will need to be changed. If a limited or qualified right is removed or affected the decision needs to be proportional and legal)*

If you have identified negative impact for any of the above characteristics, and have not been able to identify any mitigation, you MUST complete a Full Equality Impact Assessment. Please speak to the Head of Equality, Diversity and Inclusion and see the Full Equality Impact Assessment (EIA) Form on DMS

Declaration	
I am satisfied this document / activity has been satisfactorily equality impact assessed and the outcome is:	Tick one box
Continue – EIA has not identified any potential for discrimination/adverse impact, or where it has this can be mitigated & all opportunities to promote equality have been taken	☑
Justify and continue – EIA has identified an adverse impact but it is felt the policy cannot be amended. ***You must complete a Full Equality Impact Assessment (EIA) Form before this policy can be ratified***.	☐
Make Changes – EIA has identified a need to amend the policy in order to remove barriers or to better promote equality ***You must ensure the policy has been amended before it can be ratified.***	☐
Stop – EIA has shown actual or potential unlawful discrimination and the policy has been removed	☐
Name: Carol Taylor	Date: Click or tap to enter a date.

Approval & Ratification		
Policy Author:	Name: [redacted]	Job title: IG Manager
Approval Committee:	Operational IT Group	Date approved: 14/09/2022
Ratification Committee:	Digital Oversight Committee	Date ratified: 07/11/2022
Person to Review Equality Analysis:	Name: [redacted]	Review Date: 13/07/2023
Comments:	Click here to enter text.	

Alder Hey Children's NHS Foundation Trust

RM38 - RECORDS MANAGEMENT POLICY

Version number:	11.1
Name of ratifying committee:	Audit and Risk Committee
Date ratified:	23/09/2021
Name of originator/author:	[redacted], Cyber Security Manager
Name of approval committee:	Information Governance Steering Group
Date approved:	08/06/2021
Name of Executive Sponsor:	Director of Corporate Affairs
Key search words:	Clinical, Creation, Corporate, Disposal, Maintenance, Record, Retention, Use, RM38
Date issued:	September 2022
Review date:	November 2022

Quick Reference Guide - Records Management Policy

This policy sets out the Trust management arrangements of all types of clinical and corporate records. Through Information Governance mechanisms, the Trust has developed appropriate processes and procedures for the management of its records, including the secure destruction of records both physical or digital.

The policy aims to provide staff with advice and support during the lifecycle of any record created during the performance of our duties.

Key Points

- Roles and responsibilities of all staff - All staff have personal responsibility for ensuring that they comply with this policy. They must understand their responsibilities as set out in the all staff section of this policy.

- Training – Training on records management is given in the Information Governance training which is mandatory on an annual basis for all staff members.

- What is a Record? This section is important to understand what we mean by a record in that Records Management principles must be applied to patient, staff or corporate records e.g. a staff Rota or a contract or invoice.

- It is important to recognize the 5 phases of the lifecycle of a record. This will help to consider what is important at each stage.

- It is important to recognize that all records have retention periods, that is, how long as a minimum they must be held for before review for disposal.

- Corporate records audits should be conducted by areas to ensure they are aware of corporate records held and adhere to principles of record management.

Version Control, Review and Amendment Log

Version Control Table				
Version	**Date**	**Author**	**Status**	**Comment**
11.1	September 2022	Cyber Security Manager	Current	2 month extension
11	September 2021	Cyber Security Manager	Archived	Add specific reference to digital files
10	May 2020	Data Protection Officer	Archived	DPO review and update across whole Policy, incorporating previous updated versions
9	December 2019	Health Records Manager, IG Manager	Archived	Reviewed and redrafted
8	April 2019	IG Manager	Archived	Updated to reflect changes in legislation
7	January 2018	IG Manager Health Records Manager	Archived	Title edited: RM38 – Records Management Policy
6.1	July 2015	Health Records Manager, IG Manager	Archived	Addition of paragraph on record keeping audit
6	April 2015	Health Records Manager IG Manager	Archived	Reviewed and re-written
5	February 2011	Health Records Manager IG Manager	Archived	This policy has been updated to reflect new CBU structure and reporting.
4	September 2010	Health Records Manager Information Governance Co-ordinator	Archived	This policy has been changed to reflect the new reporting arrangements. The newly formed Records Management Steering Group will now monitor this policy rather than the Information Governance Steering Group.
3	February 2010	Health Records Manager IG Co-ordinator	Archived	Clinical and Corporate Records included
2	October 2006	Health Records Manager IG Co-ordinator	Archived	
1	March 2004	Unknown	Archived	

Disposal of Records Policy – RM39				
1	January 2006	Bernie Aldridge	Archived	Incorporated into Records Management Policy
0	April 2004	Unknown	Archived	

Security of Case Notes when Away from Medical Records Policy – RM40

1	March 2004	Paula Thomas	Archived	Incorporated into Records Management Policy

Case Note Tracking – RM41				
1	March 2004	Bernie Aldridge	Archived	Incorporated into Records Management Policy

Record Keeping – C22				
1	February 1998	Unknown	Archived	Incorporated into Records Management Policy

Record of changes made to Records Management Policy – Version 11.1			
Section Number	**Page Number**	**Change/s made**	**Reason for change**
All	All	Dates updated	2 month extension to complete ratification process

Record of changes made to Records Management Policy – Version 11			
Section Number	**Page Number**	**Change/s made**	**Reason for change**
Various	Various	Add specific reference to digital files	Updated

It is the responsibility of the staff member accessing this document to ensure that they are always reading the most up to date version. This will always be the version on the Document Management System.

Contents

1 Introduction

1.1 The Trust is responsible under the Public Records Acts, the Data Protection Act 2018 in conjunction with the General Data Protection Regulation (GDPR) and the Freedom of Information Act 2000 to ensure that all records, digital and paper, personal or non-personal, are created, maintained, used and disposed of in line with the requirements of these Acts.

1.2 This policy will set the standards for meeting the Trust's business needs, ensure conformance to relevant legislation, regulations and standards, and provide a basis for accountability and responsibilities for information and records management, linking with Corporate Governance and, as such, provides Board assurance:

- To provide 'best practice' guidelines for record keeping for the Trust staff, for both digital and paper records;
- To adopt and comply with the Records Management Code of Practice for Health and Social Care 2016; and
- To ensure that security and confidentiality of the Trust's records (both digital and paper) are maintained.

1.3 Where appropriate, we will follow accepted international standards such as ISO 27001 and/or ISO 22301.

2 Purpose

2.1 This document sets out the Trust's policy regarding all types of clinical and corporate records. The Trust will develop (through its Information Governance (IG) mechanisms), appropriate processes and procedures for the management of its records, including the secure destruction of records.

2.2 A crucial component of managing information is knowing what information is held and its purpose, and this forms the first stage in effective information management. The Information Governance team has a process documented for the review of records held by areas – the Information Asset Register. This can be found on the Trust Intranet Information Governance page.

2.3 Whilst this policy forms part of the requirements of the Data Security and Protection Toolkit, it is also an important component in guiding employees on security of Person Identifiable Information (PII) and the use of information in accordance with the Data Protection Act and the Freedom of Information Act.

2.4 This over-arching policy provides the basis for good information lifecycle and records management. It covers all health and non-health information, person / patient identifiable information, and records of all types including corporate information regardless of the media on which they are held.

3 Definitions

3.1 Active Records

Records necessary for conducting the current and ongoing business of an organisation.

3.2 Archives

Those records that are appraised as having permanent value for evidence of on-going rights or obligations, for historical or statistical research or as part of the corporate memory of the organisation. (The National Archives, Records Management Standard RMS 3.1)

3.3 Authenticity

An authentic record is one that can be proven:

- To be what it purports to be;
- To have been created, or sent, by the person purported to have created or sent it; and
- To have been created or sent at the time purported.

To ensure the authenticity of records, organisations should implement and document policies and procedures which control the creation, receipt, transmission, maintenance and disposition of records to ensure that record creators are authorised and identifiable and that records are protected against unauthorised addition, deletion, alteration, use and concealment.

3.4 Authorised user

Is a member of staff or individual working on behalf of the Trust who has satisfied the required employment checks, access authentication process, and completed the required training to ensure secure and confidential access to clinical and corporate records in any format.

3.5 Breach of Confidentiality

A breach of confidentiality is the unauthorised disclosure of personal information provided in confidence.

3.6 Confidential Information

Confidential information can be anything that relates to patients, staff or any other information (such as contracts, tenders etc.) held in any form (such as paper or other forms including digital, microfilm, audio or video) howsoever stored (such as patient records, paper diaries, computer or on portable devices such as laptops, PDAs, tablets, mobile telephones, etc.) or even passed by word of mouth. Person Identifiable Information (PII) is anything that contains the means to identify an individual. For further information refer to the Trust Confidentiality Policy.

3.7 **Corporate Records**

Records (other than health records) that are of, or relating to, an organisation's business activities covering all the functions, processes, activities and transactions of the organisation and of its employees.

3.8 **Destruction**

The process of eliminating, or deleting records beyond any possible reconstruction.

3.9 **Disposal**

Disposal is the implementation of appraisal and review decisions. These comprise the destruction of records and the transfer of custody of records (including the transfer of selected records to an archive institution). They may also include the movement of records from one system to another.

3.10 **File**

An organised unit of documents, physical or digital, grouped together either for current use by the creator or in the process of archival arrangement, because they relate to the same subject, activity or transaction. A file is usually the basic unit within a records series.

3.11 **Filing Referencing System**

A plan for organising records so that they can be found when needed (The National Archives, Records Management Standard RMS 1.1).

3.12 **Integrity of Records**

The integrity of a record refers to its being complete and accurate. It is necessary that a record be protected against unauthorised alteration. Records management procedures should specify what additions or annotations may be made to a record after it is created, under what circumstances additions or annotations may be authorised and who is authorised to make them. Any unauthorised annotation, addition or deletion to a record should be explicitly identifiable and traceable.

3.13 **Person Identifiable Information (PII)**

Key identifiable information includes:

- Name, address, full post code, date of birth;
- Pictures, photographs, videos, audio-tapes or other images of patients or staff;
- Alder Hey number, NHS number and local patient identifiable codes;
- Anything else that may be used to identify a patient directly or indirectly. For example, rare diseases, drug treatments or statistical analyses which have very small numbers within a small population which may allow individuals to be identified.

3.14 Public Records

Records as defined in the Public Records Act 1958 or subsequently determined as public records by The National Archives. Records of NHS organisations (and those of predecessor bodies to NHS organisations) are defined as public records under the terms of the Public Records Act 1958 sections 3(1)–(2). NHS records are not owned by the NHS organisation that created them and may not be retained for longer than 30 years without formal approval by The National Archives. Records of services supplied within NHS organisations but by outside contractors are not defined as public records, but are subject to the Freedom of Information Act.

3.15 Record

A record is anything which contains information (in any media), which has been created or gathered as a result of any aspect of the work of NHS employees, examples include:

- Patient health records (digital and paper based);
- Administrative records (e.g. personnel, estates, financial and accounting records; notes associated with complaint-handling etc.);
- X-ray and imaging reports, photographs, and other images;
- Dental moulds
- Microform (i.e. fiche/film);
- Audio and videotapes, CCTV footage, CD-ROM, DVD etc.;
- Computer databases, output, portable storage media and all other digital records;
- E-mails and text messages; and
- Material intended for short term or transitory use, including notes and ‘spare copies’ of documents.

NB: This list is not exhaustive.

3.16 Records Lifecycle

The term Records Lifecycle describes the life of a record from its creation/receipt through the period of its ‘active’ use, then into a period of ‘inactive’ retention (such as closed files which may still be referred to occasionally) and finally either confidential disposal or archival preservation.

4 Roles and Responsibilities

4.1 Chief Executive

The Chief Executive has overall responsibility for records management in the Trust. As accountable officer, they are responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity. Records management is key to this as it will ensure appropriate, accurate information is available as required.

The Trust has a particular responsibility for ensuring that it corporately meets its legal responsibilities, and for the adoption of internal and external governance requirements.

4.2 Senior Information Risk Officer (SIRO)

The Senior Information Risk Officer (SIRO) has Board level responsibility for Information Governance (IG). The SIRO has responsibility for overseeing the Information Governance framework and managing information risk across the organisation. This position is assigned by the Trust Board.

4.3 Caldicott Guardian

The Trust's Caldicott Guardian has a particular responsibility for reflecting patients' interests regarding the use of patient identifiable information. The Caldicott Guardian is responsible for ensuring patient identifiable information is shared in an appropriate and secure manner. This position is assigned by the Trust Board.

4.4 Information Governance Steering Group

The Trust's Information Governance Steering Group is responsible for ensuring that this policy is implemented and that the records management system and processes are developed, co-ordinated and monitored.

4.5 Records Manager

The Records Manager is responsible for the overall development and maintenance of records management practices throughout the Trust, in particular for drawing up guidance for good records management practice and promoting compliance with this policy in such a way as to ensure the effective, efficient, appropriate and timely retrieval of patient information.

4.6 Information Governance Manager

The Information Governance Manager is responsible for co-ordination of the Information Governance agenda, completion and submission of the Data Security and Protection Toolkit, co-ordination of mandatory Information Governance training and general awareness raising and engagement of staff in relation the Data Protection Act and the General Data Protection Regulation.

4.7 Associate Chief Operating Officers / Heads of Corporate Function

The responsibility for local records management is devolved to the relevant Directors, Associate Chief Operating Officers and Heads of Corporate Function, who may also be the designated Information Asset Owner. They will have overall responsibility for the management of records generated by their operational activities, i.e. for ensuring that records controlled within their function are managed in a way which meets the aims of the Trust's Records Management Policy.

4.8 Information Asset Owner (IAO)

IAOs are directly accountable to the SIRO and will provide assurance that information risk is being managed effectively for their assigned information assets. IAOs may be assisted in their roles by staff acting as Information Asset Administrators (IAA), or persons with equivalent responsibilities, who have day to day responsibility for management of information risks affecting one or more

assets. IAOS or IAAs are required to undergo IAO training on responsibilities within their role every three years.

4.9 All Staff

All Trust staff, whether clinical or administrative, who create, receive and use records have records management responsibilities. In particular all staff must ensure that they keep appropriate records of their work in the Trust and manage those records in keeping with this policy and with any guidance subsequently produced.

All staff must understand that information held by Trust must be used only for the intentions for which it was created and never for an individual employee's personal gain or purpose.

All staff have a responsibility to attend information Governance Mandatory training on an annual basis in which Records Management principles are covered.

5 Legal and Professional Obligations

5.1 Public Records Act

Records of NHS organisations are public records in accordance with Schedule 1 of the Public Records Act 1958. This includes records controlled by NHS organisations under contractual or other joint arrangements, or as inherited legacy records of defunct NHS organisations. This applies regardless of the records format. Principle legislation and standards in relation to this policy are:

- General Data Protection Regulation (GDPR)
- Data Protection Act 2018
- Freedom of information Act 2000
- Public Records Act 1958
- Records Management Code of Practice for Health and Social Care 2016
- Caldicott Report 1997 and subsequent reviews 2014 and 2016
- Relevant professional record keeping standards e.g. NMC, GMC
- NHS Constitution

6 Business Requirements

6.1 Records Management Key Requirements

The key requirements of this policy are that:

- **Records are available when needed** - from which the Trust is able to form a reconstruction of activities or events that have taken place;
- **Records can be accessed** - records and the information within them can be located and displayed in a way consistent with its initial use,

and that the current version is identified where multiple versions exist;

- **Records can be interpreted** - the context of the record can be interpreted: who created or added to the record and when, during which business process, and how the record is related to other records;
- **Records can be trusted** – the record reliably represents the information that was actually used in, or created by, the business process, and its integrity and authenticity can be demonstrated;
- **Records can be maintained through time** – the qualities of availability, accessibility, interpretation and trustworthiness can be maintained for as long as the record is needed, perhaps permanently where required, despite changes of format;
- **Records are secure** - from unauthorised or inadvertent alteration or erasure, that access and disclosure are properly controlled and audit trails will track all use and changes. To ensure that records are held in a robust format which remains readable for as long as records are required;
- **Records are retained and disposed of appropriately** - using consistent and documented retention and disposal procedures, which include provision for appraisal and the permanent preservation of records with archival value; and
- **Staff members are trained** - so that all staff are made aware of their responsibilities for record-keeping and record management.

6.2 This policy relates to all clinical and non-clinical records held in any format by the Organisation. These include those pertaining to:

- Patient notes
- Personnel or HR records including those pertaining to pensions
- Records of financial matters such as accounts, expenses and payroll
- Contractual matters including those with commissioners
- Marketing and publicity
- Performance information including local and national data submissions
- Conduct of affairs
- Administrative records including e.g. diaries, lists, emails, correspondence
- Estates
- Complaints
- Significant events
- Risk

- Litigation records
- Safeguarding records
- Documentation associated with meetings including Terms of Reference and Minutes
- All corporate information listed on the Information Asset Register

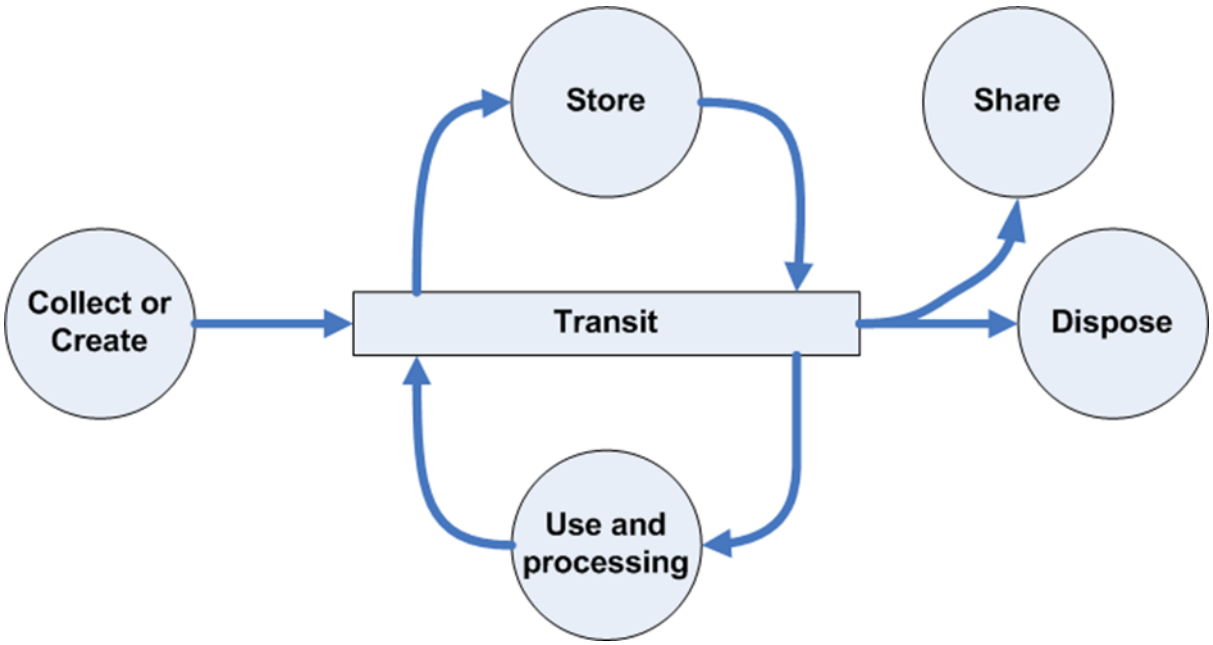
7 The 5 Phases of the Information Lifecycle

The information lifecycle defines 5 distinct phases:

1. Creation
2. Retention
3. Maintenance
4. Use
5. Disposal

This policy covers the details for each of these phases and the Trust's employees' obligations under this policy. This policy also covers the obligations of all organisations contracted to the Trust, and any organisation or third party, who share Person Identifiable Information within the Trust.

Information lifecycle is set out in the following diagram:



7.1 **Creation:** When creating information in the first instance, the following should be adhered to. The information must be:

- 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;

- 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/retained.

Employees should consider the following when creating information:

- What they are recording and how it should be recorded;
- Why they are recording it;
- How to validate information (e.g. with the patient or carers or against other records) to ensure they are recording the correct data;
- How to identify and correct errors and how to report errors if they find them;
- Staff should also understand what the records are used for and therefore why timeliness, accuracy and completeness of recording is so important; and
- How to update information, and how to add in information from other sources.

7.2 **Retention:** Retention periods refer to how long we need to keep records for.

Article 5(1)(e): Storage Limitation under GDPR states that:

1. Personal data shall be:

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational

measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')

This means that we should:

- Review the length of time we keep personal data;
- Consider the purpose or purposes we hold the information for in deciding whether (and for how long) to retain it;
- Securely delete information that is no longer needed for this purpose or these purposes; and
- Update, archive or securely delete information if it goes out of date.

The Data Protection Act does not state minimum or maximum retention periods, however, the **Records Management Code of Practice for Health and Social Care 2016** details an updated retention schedule.

Appendix 3 of the Code of Practice 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.

As delegated legislation from the Government, all Health and Social Care providers must follow the Code of Practice.

The retention period for a record varies dependant on the type of information being stored in it. The Trust maintains its own records retention schedules based on the Code of Practice and also relevant Trust business needs.

Medical records in relation to tissues and / or cells which are stored, are retained for 30 years as required by Human Tissue Authority (HTA) in accordance with directions 002/2018 following the use, expiry or disposal of tissues and / or cells to ensure traceability. Traceability refers to the completeness of auditable information about every step in the pathway for the use of relevant material, from consent through to disposal or use of the tissue to extinction. Documented records are used by licensed and unlicensed establishments to evidence traceability and ensure a robust audit trail.

When considering retention of records, it must be remembered that any record created during the performance of a member of staffs' duties is a public record and could be subject to requests for information under the Data Protection Act or Freedom of Information Act. Failure to apply retention periods set by the Trust or nationally could lead to enforcement action from the Information Commissioners Office (ICO):

- If we destroy the record before the minimum amount of time we are required to keep it - Failure to retain the record within the appropriate Trust or national retention periods could mean that we are unable to provide the record under these requests which could lead to an enforcement notice or a monetary penalty notice from the Information Commissioners Office under the Data Protection Act and General Data Protection Regulation (GDPR).

- If we keep hold of the record for longer than we need to we need to either justify a business / clinical need to retain the information or this may lead to an enforcement notice or a monetary penalty notice from the Information Commissioners office under the Data Protection Act and General Data Protection Regulation (GDPR).

For guidance on review of records including retention periods visit the link from the NHS Digital site for the Records Management Code of Practice for Health and Social Care 2016.

7.3 **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. The use of standardised filenames and version control methods should be applied consistently throughout the life of the information.

All areas have responsibility to determine whether records are appropriately held. In order to do this an audit should be conducted, using records review documentation, to determine:

- Retention periods - are these being adhered to or documented where records are held outside of this.
- Storage - are storage arrangements appropriate and secure.
- Relevant to area - do the records need to be held by this area or is it more appropriate for them to be held by another area.
- Disposal - appropriate disposal once retention periods are reached.

Consideration for Scanning - for reasons of business efficiency, or in order to address problems with storage, consideration should be given of the option of scanning into digital format, records which currently exist in paper format. When scanning there is a need to protect the evidential value of the record by copying and storing the record in accordance with the section on Scanned Records, in the Records Management Code of Practice for Health and Social Care 2016.

In order to fully realise the benefits of reduced storage requirements and business efficiency, the information owners should consider disposing of paper records that have been copied into digital format and stored in accordance with appropriate standards.

For guidance on how to appropriately maintain records and how to conduct a corporate records audit visit the Information Governance Page of the Intranet and follow the review of records link.

7.4 **Use:** All information must be used consistently, only for the intentions for which it was created and never for an individual employee’s personal gain or purpose as stated in the Trust Data Protection Policy.

- **Disclosure** - only the specific information required should be disclosed to authorised parties and always in accordance and with strict adherence to the Data Protection Act and General Data Protection Regulation (GDPR). There are a range of statutory provisions that limit, prohibit or set conditions in respect of the disclosure of records to third parties, and similarly, a range of provisions that require or permit disclosure. Advice from NHS DIGITAL in the form of a guide to confidentiality within the NHS and social care is available from the NHS Digital page.

- **Transfer** – The mechanisms for transferring information from one organisation to another should also be tailored to the sensitivity of the material contained within the records and the media on which they are held. All transfers of digital personal or sensitive (special category) data must be transferred using encryption technology.

- **Closure** – Information held in records should be closed as soon as they have ceased to be in active use other than for reference purposes. An indication that a file of paper records, or folder of digital records, has been closed, together with the date of closure, should be shown on the record itself as well as noted in the index or database of the files / folders. Where possible, information on the intended disposal of digital records should be included in the metadata when the information is created. The storage of closed records should follow accepted standards relating to environment, security and physical organisation of the files.

7.5 **Disposal:** It is particularly important under both Data Protection and Freedom of Information legislation that the disposal of records, which is defined as the point in their lifecycle when they are either transferred to an archive or destroyed, is undertaken in accordance with clearly established policies which have been formally adopted by the Trust and which are enforced by properly trained and authorised staff.

- **Disposed of appropriately** - using consistent and documented retention and disposal procedures, which include provision for appraisal and the permanent preservation of information with archival value. Information lifecycle management is the responsibility of all staff and therefore managers are responsible for ensuring weeding exercises to review information held within departments are undertaken on a regular basis.
- **Destroyed appropriately** - records can contain sensitive or confidential information. It is therefore vital that confidentiality is safeguarded at every stage and that the method used to destroy records is fully effective and secures their complete illegibility and inability to be reconstructed. Any records that have been identified for destruction must be destroyed as soon as possible after they are eligible.

8 Pre-adoption Medical Records

It is likely that some of the pre-adopted records may be provided to the data subject / applicant. This is on the basis that much of the content of the medical records will already have been pulled into the new post adoption medical record.

This medical information would already be readily available to an adopted child / parent, and is unlikely to contain sensitive information concerning the adoption, which would be kept by adoption agencies.

The pre-adoption medical records could be made available to the adoptive parents, once you are satisfied as to the identity and parental responsibility of the applicant for the child, who is confirmed as unable to consent for themselves.

Redactions / information withheld should be applied in the normal way under GDPR / DPA principles, such as where there is third party data or the data would be likely to cause serious harm to the physical or mental health of the data subject or another individual.

In addition, and with very careful review, and additional review from somebody else, anything held that relates to the adoption in any way should be redacted. This could include, for example, previous names, addresses and unique numbers of the child, if they are not already known to the adoptive parents.

9 Training

9.1 Training in relation to Records Management is given in Information Governance training which is mandatory on an annual basis for all staff.

Support and guidance on any of the stages of Records Management will be offered by a number of methods by the Records Manager and Information Governance Manager. Areas / Team meetings can be visited to provide advice and support this process.

10 Monitoring

10.1 Information Governance spot checks will incorporate review of areas relating to Records Management e.g. appropriate storage of records / physical security of records / retention of records and will provide assurance of compliance with policy.

10.2 Results of audits will be reported to the Information Governance Steering Group.

10.3 Support and guidance on any of the stages of Records Management will be offered by a number of methods by the Records Manager and Information Governance Manager. Areas / Team meetings can be visited to advise and support this process. The Intranet Information Governance Pages are the main information portal in relation to this subject.

Key Performance Indicator	Schedule of monitoring	Monitoring conducted by whom	Form of monitoring	Findings of monitoring reported to
Data Security and Protection Toolkit.	Annual	Information Governance Manager	Action Plan	Information Governance Steering Group (IGSG)
A serious breach must be reported to the Information Commissioner's Office (ICO) within 72 hours. When a serious breach occurs this can result in the Trust being investigated and potentially fined by the ICO.	Annual	Information Governance Manager	Review of incident with findings and recommendations from the ICO	Information Governance Steering Group (IGSG)
Review suite of other policies and standards around Data Protection and IT Security policies.	Annual	Information Governance Manager	Version Control	Information Governance Steering Group (IGSG)

11 Further Information

Related Policies

- E-mail and Internet Policy – M24
- Incident Reporting Policy – RM2
- Data Protection and Confidentiality Policy– RM44
- Freedom of Information Policy – M25
- Data Quality Policy – RM45
- Information Security Policy – RM42
- Information Governance Policy - M45
- Records Management Standard Operating Procedures

Equality Analysis (EA) for Policies		
The Public Sector Equality Duty (section 149 of the Equality Act 2010) requires public authorities to have due regard for the for need to achieve the following objectives in carrying out their functions: a) Eliminate discrimination, harassment, victimisation and any other conduct that is prohibited by or under the Equality Act 2010. b) Advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it c) Foster good relations between persons who share a relevant protected characteristic and persons who do not share it. Please refer to Equality Analysis Step-Wise Guide for Policies when completing this form		
Policy Name	Records Management Policy	
Policy Overview	This Policy is part of a suite of data protection policies now aligned to the updated legislation – the General Data Protection Regulation 2016 and the Data Protection Act 2018.	
Relevant Changes (if any)	To bring into annual review	
Equality Relevance Select LOW, MEDIUM or HIGH	LOW	
If the policy is LOW relevance, you **MUST** state the reasons here.	The purpose of the policy is to provide guidance and details of staff responsibilities in order to comply with legislation. Therefore, having considered the equality implications of the policy, they are of low relevance.	
Form completed on:	Date: 08/09/2021	
Form completed by:	Name: [redacted]	Job Title: Cyber Security Manager

Approval & Ratification of Equality Analysis		
Policy Author:	Name: [redacted]	Job title: Cyber Security Manager
Approval Committee:	Information Governance Steering Group	Date approved: 08/06/2021
Ratification Committee:	Audit and Risk Committee	Date ratified: 23/09/2021
Person to Review Equality Analysis:	Name: [redacted]	Review Date: 23/09/2024
Comments:	Click here to enter text.	