NHS
Mersey Care
NHS Foundation Trust

Community and Mental Health Services

TRUST-WIDE NON - CLINICAL POLICY

CORPORATE RECORDS

Policy Number:	**IT04**
Scope of this Document:	**All Staff**
Recommending Committee:	**Joint SIRO and Information Governance Group**
Approved By:	**Executive Director of Finance**
Date Ratified:	**June 2020**
Next Review Date (by):	**May 2021**
Version Number:	**2020 – Version 8**
Lead Executive Director:	**Executive Director of Finance**
Lead Author(s):	**Medical Director/Caldicott Guardian**

TRUST-WIDE NON- CLINICAL POLICY

2020 – Version 8

Striving for perfect care and a just culture

TRUST-WIDE NON- CLINICAL POLICY

CORPORATE RECORDS

Further information about this document:

Document name	**IT04 – CORPORATE RECORDS**
Document summary	**This policy defines the framework to ensure the Trust meets its obligations in relation of Information Governance and Records Management. This policy is issued as guidance on the creation, storage and management of Corporate Records.**
Author(s) Contact(s) for further information about this document	**Geoff Springer** **Information Governance Officer** **Tel: 0151 478 6899** **Email:geoff.springer@merseycare.nhs.uk**
Published by Copies of this document are available from the Author(s) and via the trust's website	**Mersey Care NHS Foundation Trust** **V7 Building** **Kings Business Park** **Prescot** **Merseyside** **L34 1PJ** **Trust's Website www.merseycare.nhs.uk**
To be read in conjunction with	**IT02 – IM&T Security Policy** **IT12 – Information Governance Policy** **IT13 – Freedom of Information Policy** **HR10 – Equality & Human Rights Policy** **General Data Protection Regulation 2018** **Data Protection Act 2018**
This document can be made available in a range of alternative formats including various languages, large print and braille etc	

Version Control:

		Version History:
Version 1	Corporate Document Review Group	March 2012
Version 2	Corporate Document Review Group	September 2014
Version 3	Corporate Document Review Group	February 2016
Version 4	Corporate Document Review Group	August 2017
Version 5	Policy Group/Executive Committee	August 2018
Version 6	Policy Group/Executive Committee	June 2019
Version 7	Policy Group/Executive Committee	July 2019
Version 8	Executive Director of Finance Approval	July 2021

SUPPORTING STATEMENTS

this document should be read in conjunction with the following statements:

SAFEGUARDING IS EVERYBODY'S BUSINESS

All Mersey Care NHS Foundation Trust employees have a statutory duty to safeguard and promote the welfare of children and adults, including:

- being alert to the possibility of child / adult abuse and neglect through their observation of abuse, or by professional judgement made as a result of information gathered about the child / adult;
- knowing how to deal with a disclosure or allegation of child /adult abuse;
- undertaking training as appropriate for their role and keeping themselves updated;
- being aware of and following the local policies and procedures they need to follow if they have a child / adult concern;
- ensuring appropriate advice and support is accessed either from managers, *Safeguarding Ambassadors* or the trust's safeguarding team;
- participating in multi-agency working to safeguard the child or adult (if appropriate to your role);
- ensuring contemporaneous records are kept at all times and record keeping is in strict adherence to Mersey Care NHS Foundation Trust policy and procedures and professional guidelines. Roles, responsibilities and accountabilities, will differ depending on the post you hold within the organisation;
- ensuring that all staff and their managers discuss and record any safeguarding issues that arise at each supervision session

EQUALITY AND HUMAN RIGHTS

Mersey Care NHS Foundation Trust recognises that some sections of society experience prejudice and discrimination. The Equality Act 2010 specifically recognises the *protected characteristics* of age, disability, sex, race, religion and belief (or lack thereof), sexual orientation, gender reassignment, pregnancy and maternity and marital and civil partnership status. The Equality Act also requires regard to socio-economic factors.

The trust is committed to promoting and advancing equality and removing and reducing discrimination and harassment and fostering good relations between people that hold a protected characteristic and those that do not both in the provision of services and in our role as a major employer. The trust believes that all people have the right to be treated with dignity and respect and is committed to the elimination of unfair and unlawful discriminatory practices.

Mersey Care NHS Foundation Trust also is aware of its legal duties under the Human Rights Act 1998. Section 6 of the Human Rights Act requires all public authorities to uphold and promote Human Rights in everything they do. It is unlawful for a public authority to perform any act which contravenes the Human Rights Act.

Mersey Care NHS Foundation Trust is committed to carrying out its functions and service delivery in line the with a Human Rights based approach and the FREDA principles of **F**airness, **R**espect, **E**quality **D**ignity, and **A**utonomy

CONTENTS

1. PURPOSE

1.1 Corporate Records Management ensures that one of the Trusts most important assets, information, is respected and held in secure and manageable conditions and the Trust can comply with its Records Management duties to comply with current legislation. It is therefore of paramount importance to ensure that corporate records and the information they contain are efficiently managed on the basis of the HORUS categorisation:

- Held safely and confidentially
- Obtained fairly and effectively
- Recorded accurately and reliably
- Used effectively and ethically
- Shared appropriately and lawfully

2. RATIONALE

2.1. The term `corporate records' means all other records held in the Trust which are not health records. The public have a right to access corporate records and information, subject to certain exemptions, under the Freedom of Information Act. This came into force on 1st January 2005. Departments who receive requests must pass them onto the Communications Team without delay as the Trust has 20 working days in which to respond. The Trust Communications Team will co-ordinate a response with final sign off by the Senior Information Risk Owner. See Trust Freedom of Information Policy for further information.

3 SCOPE

3.1 This policy applies to all staff who create any corporate record within the organisation. This policy covers all aspects of information use within the organisation, including but not limited to:-

- Personnel information/human resources
- Organisational Information
- Estates/Engineering
- Financial
- IM&T
- Purchasing / supplies

The policy covers all aspects of processing information in relation to:-
- Structured record systems-paper and electronic

4 OUTCOME & OBJECTIVES

4.1 **Electronic corporate records**
Corporate information refers to information generated by an organisation other than clinical (or service user) information. The term describes the records generated by an organisation's business activities, and therefore will include records from the following (and other) areas of the Trust:

4.1.1 Electronic corporate records must be accessible and retrievable when and where required. It is NOT only concerned with corporate records that are part of a formal electronic document and record management system (EDRMS), but includes records on network drives and in shared folders. Emails and attachments, and web pages on Internet and Intranet sites are considered corporate records. When handling any type of record, it is important to make the distinction between a record and a document. A document becomes a record when it has been finalised and become part of an organisation's corporate information. At this point, the record should not be amended and should only be held in the corporate system, e.g. the network drive, shared folder or EDRMS, and not on a local drive on a PC or laptop. Due to the nature of electronic documents, it is vital that a process of version control is in place, so that changes are recognisable and taken into account during any decision making process.

4.1.2 Electronic records must be maintained in a system that ensures they are properly stored and protected throughout their life cycle, including their migration across systems.

4.1.3 Ideally, the electronic record systems in place should:

- Provide audit trails to accurately log when records are created, accessed or disposed of;
- Have a logical filing structure to enable the quick and efficient filing and retrieval of records when required and enable implementation of authorised disposal arrangements, i.e. archiving, migration to another format or destruction;
- Control access to records through a variety of security measures, including user verification, password protection and access monitoring where appropriate;
- Support technological upgrades to ensure records remain accessible and usable throughout their life cycle;
- Permit cross-referencing of electronic records to their paper counterparts (where dual systems are maintained).
- All final documents must be Trust branded and be on corporate templates, please see Trust Policy on Policy Development.

5. PROCESS

5.1 Referencing

5.1.1 The referencing system should meet the business needs, and be easily understood by staff members that create electronic documents and records.

5.1.2. Several types of referencing can be used, e.g:-alphanumeric; alphabetical; numeric; keyword.

5.1.3. The most common of these is alphanumeric, as it allows letters to be allocated for a business activity, e.g. HR for Human Resources, followed by a unique number for each electronic record or document created by the HR function. It may be more feasible in some circumstances to give a unique reference to the file or folder in which the record is kept and identify the record by reference to date and format.

5.2 **Naming**

5.2.1 Also known as file naming conventions, the National Archives offers the following advice:

- Give a unique name to each record;
- Give a meaningful name which closely reflects the records contents;
- Express elements of the name in a structured and predictable order;
- Locate the most specific information at the beginning of the name and the most general at the end;
- Give a similarly structured and worded name to records which are linked (for example, an earlier and a later version).

5.3 **Filing structure**

5.3.1 Clear and logical filing structures that aid retrieval of records should be used. Ideally, the filing structure should reflect the way in which paper corporate records are filed to ensure consistency. However, if it is not possible to do this, the names allocated to files and folders should allow intuitive filing. Filing of corporate records to local drives on PCs and laptops is strongly discouraged.

5.4 **Paper corporate records**

5.4.1 **Filing structure**

5.4.2 Clear and logical filing structure that aids retrieval of records should be used. Ideally, the filing structure should reflect the way in which paper corporate records are filed to ensure consistency. However, if it is not possible to do this, the names allocated to files and folders should allow intuitive filing.

5.4.3 Robust tracking / tracing processes must be in place, which enable the movement and location of records to be controlled and provide an auditable trail of record transactions. The process need not be a complicated one, e.g. a book that staff members sign when a corporate record is removed or returned might be appropriate. A document becomes a record when it has been finalised and become part of an organisation's corporate information. With paper records, a further distinction must be made between the original record and a copy of that record.

5.4.4 The original record should only be held in the corporate recordkeeping system, and not in staff desk drawers, etc. Ideally, a paper record-keeping system should ensure that:

- Logs are kept to accurately document when records are created (i.e. the date that a document becomes a formal corporate record), accessed (e.g. a sign-out book) and disposed of;
- Records are grouped in a logical structure to enable the quick and efficient filing and retrieval of information when required and enable implementation of authorised disposal arrangements, i.e. archiving or destruction;
- Suitable storage areas are used to ensure records remain accessible and usable throughout their life cycle;
- Access to records is controlled through a variety of security measures, e.g. authorised access to storage and filing areas, lockable storage areas;
- Issue from and return to storage areas on site or to authorised off-site facilities is documented.

5.5 Referencing

5.5.1 Referencing systems should meet the business needs, and be easily understood by staff members that create, file or retrieve paper records. Several types of referencing can be used, e.g. alphanumeric; alphabetical; numeric; keyword. The most common of these is alphanumeric, as it allows letters to be allocated for a business activity, e.g. ES for Estates, followed by a unique number for each record created by the Estates function. It may be more feasible in some circumstances to give a unique reference to the file in which the record is kept and identify the record by reference to date and format.

5.6 Naming

5.6.1 Also referred to as file naming conventions. The National Archives offers the following advice:

Give a unique name to each record;
Give a meaningful name which closely reflects the record contents;
Express elements of the name in a structured and predictable order;
Locate the most specific information at the beginning of the name and the most general at the end;
Give a similarly structured and worded name to records which are linked (for example, an earlier and a later version).

5.7 Indexing and filing

5.7.1 The index (or register) is primarily a signpost to where paper corporate records are stored, e.g. the relevant folder or file. However, it can also be a guide to the information contained in those records. The index should be arranged in a user-friendly structure that aids easy location and retrieval of a folder or file. Folders and files should be given clear and logical names to assist filing and retrieval of records. Filing of corporate records in desk drawers should not happen.

5.8 Classification marking guidance (Department of Health)

5.8.1 This NHS Information Governance (IG) guidance is provided as good practice for NHS organisations of all types to consider in marking the records for which they are responsible. It is applicable to both information recorded on paper and that processed electronically including printouts, reports etc. Through the application of this guidance, NHS organisations should be able to further demonstrate the effectiveness of their local IG practices. This guidance should be considered alongside other published NHS IG Codes of Practice and guidance for Confidentiality, Records Management, Information Security Management, Legal and Professional obligations. These are currently available for download through the Department of Health website at www.dh.gov.uk.

5.8.2 There has previously been no single or consistent system of classification marking of information within the NHS. Many NHS bodies have adopted their own classification schemes and this can cause confusion when organisations merge or where information is shared between organisations. This is particularly marked where, as in the case of, for example, NHS and Social Care organisations, there may be a need for common assurances in information partnerships. There is also danger of a lack of consistency in data handling and retention practice when information is shared with non-NHS bodies that relate to several NHS

organisations. The lack of a single coherent system also hampers the development of appropriate IT system protocols for the NHS.

5.9 Background and classification scheme outline

5.9.1 This guidance paper sets out a proposed simple scheme of classification relevant to the needs of NHS organisations and for the common benefit of all. It is similar to that used in central Government and other public sector organisations but takes account of important differences in the nature of NHS business activity and the kind of information used between the NHS and other public sector environments. Equally, the NHS does not have a requirement for the full range of protective markings used in Government. For example, central Government uses six categories of information classification, two of which - Secret and Top Secret - are, usually, only relevant to a very limited number of very serious situations involving national security and economic stability. The others are Confidential, Restricted, Protect and Unclassified. These are more relevant within an NHS context and are terms that were considered in developing this classification guidance. Categories proposed for use are prefixed "**NHS**" to indicate their relevance to a particular environment. NHS information that has no classification requirement should be considered **Unclassified** and may optionally be marked as such.

5.10 NHS Confidential

5.10.1 In Government, the marking "Confidential" would, for example, denote information that could undermine the viability of national organisations, damage security operations or national finances or economic and commercial interests. These considerations are unlikely to apply in an NHS context. But within the NHS it is generally recognised, and there is a substantial body of case law that requires, that person-identifiable clinical information should always be held confidentially (*Confidentiality*: NHS Code of Practice). Therefore, the marking **NHS CONFIDENTIAL** should be used for that kind of information (e.g. patients' clinical records, patient identifiable clinical information, and information about NHS staff that passes between NHS staff, and between NHS staff and staff of other appropriate agencies). This will include patient demographic details that might identify people who have had a GP contact/hospital appointment within a particular timeframe or who may have a particular condition. (**NOTE**: In order to safeguard confidentiality, the term "NHS Confidential" should **never** be used on correspondence to a patient.)

5.10.2 The endorsement **NHS CONFIDENTIAL** should be included at the top centre of every page of the document. Documents so marked should be held securely at all times. That is, they should be stored in a locked room or equivalently within secured electronic systems to which only authorised persons have access. They should not be unattended at any time in any place where unauthorised persons might gain access to them. They should be transported securely in sealed containers and not unattended at any stage. Documents marked NHS CONFIDENTIAL not in a safe store or transport should be kept out of sight of visitors or others not authorised to view them.

5.11 Other uses of NHS Confidential

5.11.1 The endorsement **NHS CONFIDENTIAL** should also be used to mark all other sensitive information. That is, material the disclosure of which is likely to:

- Adversely affect the reputation of the organisation or it's officers or cause substantial distress to individuals;
- Make it more difficult to maintain the operational effectiveness of the organisation;
- Cause financial loss or loss of earning potential, or facilitate improper gain or disadvantage for individuals or organisations;
- Prejudice the investigation, or facilitate the commission of crime or other illegal activity;
- Breach proper undertakings to maintain the confidence of information provided by third parties or impede the effective development or operation of policies;
- Breach statutory restrictions on disclosure of information;
- Disadvantage the organisation in commercial or policy negotiations with others or undermine the proper management of the organisation and its operations.

5.11.2 A paper, printout or report etc. marked **NHS CONFIDENTIAL** may also be endorsed with a suitable descriptor indicating the reason for the classification e.g. 'NHS CONFIDENTIAL – PATIENT INFORMATION' or 'NHS CONFIDENTIAL – COMMERCIAL'.

A list of the relevant descriptors is included in **Table 1**. The endorsement should be included at the top-centre on every page of the document. **NHS CONFIDENTIAL** documents should be stored in lockable cabinets or equivalently secured electronic systems. Information may be classified **NHS CONFIDENTIAL** in the light of the circumstances at a particular time. The classification should be kept under review and the information de-classified when the need for this protection no longer applies. NHS use of an equivalent classification for "Restricted" is unnecessary when **NHS CONFIDENTIAL** is used.

5.12 NHS Protect

5.12.1 In Government a new marking of **"**PROTECT" was recently introduced. This discretional marking may be used in order to avoid unauthorised access to information. It establishes basic principles to handle with care, take relevant precautions and dispose of properly. In the NHS context, it is therefore possible for NHS organisations to adopt and use an equivalent **NHS PROTECT** marking, with or without descriptors, for information that requires protection below that of **NHS CONFIDENTIAL** and where care in handling is still necessary. NHS organisations that choose to adopt **NHS PROTECT** must therefore ensure their staff and business partners are aware of the different expectations and arrangements that apply for the protection and assurance of **NHS CONFIDENTIAL** and **NHS PROTECT** marked information.

5.13 Freedom of Information

5.13.1 When classifying NHS documents regard should be paid to the requirements of the Freedom of Information Act 2000. Careful consideration should be given before marking documents that would normally be published or disclosed on request. Over-classification might lead to an inappropriate decision not to disclose information that would later be embarrassing to the organisation (for example, where there was an appeal against non-disclosure or the Information Commissioner became involved). Protective markings should wherever possible be

restricted to information that would be exempt from disclosure, including temporary exemption – See 4.7 Table 2. Further information about the Act and its exemptions (including the drafts of documents that are intended for publication application of the "public interest" test) is available on the website of the Information Commissioner (www.informationcommissioner.gov.uk) Also see the Trust Freedom of Information Act Policy

5.14 Classification of NHS Information - Marking Guidance for NHS Organisations

5.14.1 **NHS CONFIDENTIAL** - appropriate to paper and electronic documents and files containing person identifiable **clinical** or NHS **staff** information and **other sensitive** information.

5.14.2 **NHS PROTECT** – Discretionary marking that may be used for information classified below NHS Confidential but requiring care in handling. Descriptors may also be used as required.

5.14.3 **Table 1 – Descriptors that may be used with "NHS CONFIDENTIAL" or "NHS PROTECT" marking**

Category Definition

- Appointments Concerning actual or potential appointments not yet announced.
- Barred - Where there is a statutory (Act of Parliament or European Law) prohibition on disclosure or disclosure would constitute a contempt of Court (information the subject of a court order).
- Board - Documents for consideration by an organisation's Board of Directors, initially, in private (Note: This category is not appropriate to a document that could be categorised in some other way).
- Commercial- Where disclosure would be likely to damage a (third party) commercial undertaking's processes or affairs.
- Contracts Concerning tenders under consideration and the terms of tenders accepted.
- For Publication -Where it is planned that the information in the completed document will be published at a future (even if not yet determined) date.
- Management Concerning policy and planning affecting the interests of groups of staff. (Note: Likely to be exempt only in respect of some health and safety issues).
- Patient Information Concerning identifiable information about patients
- Personal Concerning matters personal to the sender and/or recipient.
- Policy Issues of approach or direction on which the organisation needs to take a decision (often information that will later be published).
- Proceedings The information is (or may become) the subject of, or concerned in a legal action or investigation.
- Staff Concerning identifiable information about staff.

5.14.4 **Table 2 - Freedom of information act exemptions**

Category Possible Exemption [section(s) of the FOI Act]

- Appointments S 40 Personal information (may be subject to a public interest test)
- Barred S 44 Legal prohibitions on disclosure Board
- Commercial S 43 Commercial interests (subject to a public interest test)
- Contracts S 43 Commercial interests (public interest test)
- For Publication S 22 For future publication (public interest test)
- Management S 38 Endanger health and safety (public interest test)
- Personal S 40 Personal Information (may be subject to public interest test)
- Policy S 22 For future publication (public interest test)
- Proceedings S 30 Investigations and proceedings

- S 31 Law enforcement

5.15 Retention periods

5.15.1 The NHS Records Management Code of Practice for Health and Social Care (2016) contains retention periods for both health and corporate records. Records, both paper and electronic, should not be kept for longer than necessary. For a copy of the full document, contact the Trust's Data Protection Officer.

5.16 Subject access requests for corporate records

5.16.1 Under the General Data Protection Regulation/Data Protection Act 2018 individuals have a right to make a request in writing for a copy of the information held about them on computer and in some manual filing systems. This is called a subject access request. For guidance on Subject access requests please see the Trust Confidentiality and Data Sharing Policy and the General Data Protection Regulation/Data Protection Act 2018.

5.16.2 Is this a subject access request?

Determine whether the person's request is a subject access request. Any written enquiry that asks for information you hold about the person making the request (data subject) can be construed as a subject access request. Any requests for access must be in writing (you may need to assist an individual to make a request to the Trust). The written request must contain sufficient information to enable the Trust to conduct the search required e.g. Name, Address and Date of Birth. Compliance with the request is not obligatory until the Trust has been provided with adequate information and identity validation. Check with the relevant department manager that the information is not normally released as part of normal business processes. If it is releasable as part of normal business processes refer to the relevant department manager who should deal with the request. Please see The Trust Freedom of Information Act Policy, General Data Protection Regulation/Data Protection Act 2018 and the Trust's Confidentiality and Data Sharing Policy for further guidance.

6 MONITORING & REVIEW

6.1 Monitoring and review of this Policy will take place by the Joint SIRO/ Information Governance Group ensuring that an annual audit of Corporate Records is undertaken and an annual report provided to the group. The Minutes and a Chair's report following each meeting of the Committee is reported to the Executive Committee for oversight and an Annual report provided to the Board of Directors.

7 DEVELOPMENT & CONSULTATION PROCESS

7.1 This policy has been developed by the Data Protection Officer. The policy has also been reviewed by the Caldicott Guardian, Senior Information Risk Owner and the Joint SIRO/Information Governance Group.

8 DUTIES & RESPONSIBILITES

8.1 **Chief Executive**

The Chief Executive as the accountable officer is responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to comply with Information Governance and Records Management.

8.2 **Senior Information Risk Owner & Executive Director of Finance**
The Trust's Senior Information Risk Owner and Executive Director of Finance have a particular responsibility in ensuring that there is a robust framework to comply with the retention of records compliant with all relevant legislation. Members of staff working in the Trust must comply with all requirements of Information Governance: which is driven by various pieces of legislation and guidelines issued by the Department of Health, Health & Social Care Information Centre and other sources.

8.3 **Data Protection Officer**
The Data Protection Officer is responsible for ensuring that the Trust is working within the legal framework of the General Data Protection Regulation, Freedom of Information Act, NHS Code of Practice for Records Management, NHS Code of Practice for Confidentiality and Information Governance Standards. The Data Protection Officer is the designated trust representative that liaises with the Information Commissioners Office and conducts internal reviews for any Freedom of Information Act complaints.

8.4 **Joint SIRO/ Information Governance Group**
The Joint SIRO/ Information Governance Group ensures the Trust operates within the Information Governance framework and reports to the Trust Executive Committee via a bi-monthly IG Chair's report and Annual Report.

8.5 **Senior Managers**
It is the responsibility for all Senior Managers to ensure that staff work within the boundaries of the Trust policies and procedures and are aware of their responsibilities.

8.6 **All staff**
All employees of the Trust, or staff working in a voluntary capacity, agency or independent contractors must adhere to the current legislative framework and Trust policies.

9 TRAINING

The processing and management of Corporate Records forms part of the Data Security Awareness training which is mandatory and has to be completed annually by all staff. The Information Governance Officer can be consulted if any technical queries arise or additional support is required.

10 APPENDICES

Appendix 1 – Reference Documents/Retention Schedule

11 REFERENCE DOCUMENTS

11.1 Freedom of Information Act 2000
http://www.opsi.gov.uk/RevisedStatutes/Acts/ukpga/2000/cukpga_20000036_en_1

11.2 General Data Protection Regulation
https://ico.org.uk/for-organisations/guide-to-the-general-data

11.3 Code of practice on the discharge of public authorities' functions under Part 1 of the Freedom of Information Act 2000 – dealing with requests for information.
http://www.foi.gov.uk/reference/imprep/codepafunc.htm

11.4 Code of practice on the management of records Issued under section 46 of the Freedom of Information Act 2000
11.5 http://www.foi.gov.uk/reference/imprep/codemanrec.htm
11.6 Data Protection Act 2018
https://ico.org.uk/for-organisations/guide-to-the-general-data
11.7 The Records Management Code of Practice (2016)
11.8 Trust Confidentiality Code and Data Sharing Policy
11.9 General Data Protection Regulation
11.10 Trust IM&T Security Policy

Appendix 1 Retention Schedule - Corporate Records

Record Type	Retention start	Retention period	Action at end of retention period	Notes
1. Event & Transaction Records				
Clinical Audit	Creation	5 years	Review and if no longer needed destroy	
Chaplaincy records	Creation	2 years	Review and consider transfer to a Place of Deposit	See also Corporate Governance Records
Datasets released by HSCIC under a data sharing agreement	Date specified in the data sharing agreement	Delete with immediate effect	Delete according to HSCIC instruction	http://www.hscic.gov.uk/media/15729/DARS-Data-Sharing-Agreement/pdf/Data_Sharing_Agreement_2015v2%28restricted_editing%29.pdf
Destruction Certificates or Electronic Metadata destruction stub or record of clinical information held on destroyed physical media	Destruction of record or information	20 Years	Review and consider transfer to a Place of Deposit	Destruction certificates created by public bodies are not covered by an instrument of retention and if a Place of Deposit or the National Archives do not class them as a record of archival importance they are to be destroyed after 20 years.
Equipment maintenance logs	Decommissioning of the equipment	11 years	Review and consider transfer to a Place of Deposit	
Inspection of equipment records	Decommissioning of the equipment	11 Years	Review and if no longer needed destroy	

Information Governance Alliance - Records Management Code of Practice for Health and Social Care 2016

Record Type	Retention start	Retention period	Action at end of retention period	Notes
2. Telephony Systems & Services (999 phone numbers,111 phone numbers, ambulance, out of hours, single point of contact call centres).				
Recorded conversation which may later be needed for clinical negligence purpose	Creation	3 Years	Review and if no longer needed destroy	The period of time cited by the NHS Litigation Authority is 3 years
Recorded conversation which forms part of the health record	Creation	Store 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 of the record and be retained accordingly.
The telephony systems record (not recorded conversations)	Creation	1 year	Review and if no longer needed destroy	This is the absolute minimum specified to meet the NHS contractual requirement.

Record Type	Retention start	Retention period	Action at end of retention period	Notes
3. Births, Deaths & Adoption Records - (see Clinical Records)				
Local Authority Adoption Record (normally held by the Local Authority children's services)	Creation	100 years from the date of the adoption order	Review and consider transfer to a Place of Deposit	The primary record of the adoption process is held by the local authority children's service responsible for the adoption service.

Record Type	Retention start	Retention period	Action at end of retention period	Notes
4. Clinical Trials & Research **For clinical trials record retention please see the MHRC guidance at https://www.gov.uk/guidance/good-clinical-practice-for-clinical-trials**				
Advanced Medical Therapy Research Master File	Closure of research	30 years	Review and consider transfer to a Place of Deposit	See guidance at: https://www.gov.uk/guidance/advanced-therapy-medicinal-products-regulation-and-licensing
Clinical Trials Master File of a trial authorised under the European portal under Regulation (EU) No 536/2014	Closure of trial	25 years	Review and consider transfer to a Place of Deposit	For details please see: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.158.01.0001.01.ENG
European Commission Authorisation (certificate or letter) to enable marketing and sale within the EU member states area	Closure of trial	15 years	Review and consider transfer to a Place of Deposit	For details please see: http://ec.europa.eu/health/files/eudralex/vol2/a/vol2a_chap1_2013-06_en.pdf
Research data sets	End of research	Not more than 20 years	Review and consider transfer to a Place of Deposit	For details please see: http://tools.jiscinfonet.ac.uk/downloads/bcsrrs/managing-research-records.pdf
Research Ethics Committee's documentation for research proposal	End of research	5 years	Review and consider transfer to a Place of Deposit	For details please see: http://www.hra.nhs.uk/resources/research-legislation-and-governance/governance-arrangements-for-research-ethics-committees/ Data must be held for sufficient time to allow any questions about the research to be answered. Depending on the type of research the data may not need to be kept once the purpose has expired. For example data used for passing an academic exam may be destroyed once the exam has been passed and there is no further academic need to hold the data. For more significant research a Place of Deposit may be interested in holding the research. It is best practice to consider this at the outset of research as orphaned personal data can inadvertently cause a data breach

Research Ethics Committee's minutes and papers	Year to which they relate	Before 20 years but as soon as practically possible	Review and consider transfer to a Place of Deposit	Committee papers must be transferred to a Place of Deposit as a public record: http://www.hra.nhs.uk/resources/research-legislation-and-governance/governance-arrangements-for-research-ethics- committees/
Record Type	**Retention start**	**Retention period**	**Action at end of retention period**	**Notes**
5. Corporate Governance				
Board Meetings	Creation	Before 20 years but as soon as practically possible	Transfer to a Place of Deposit	Board Meetings
Board Meetings (Closed Boards)	Creation	May retain for 20 years	Transfer to a Place of Deposit	Although they may contain confidential or sensitive material they are still a public record and must be transferred at 20 years with any FOI exemptions noted or duty of confidence indicated.
Chief Executive records	Creation	May retain for 20 years	Transfer to a Place of Deposit	This may include emails and correspondence where they are not already included in the board papers and they are considered to be of archival interest.
Committees Listed in the Scheme of Delegation or that report into the Board and major projects	Creation	Before 20 years but as soon as practically possible	Transfer to a Place of Deposit	Committees Listed in the Scheme of Delegation or that report into the Board and major projects
Committees/ Groups / Sub-committees not listed in the scheme of delegation	Creation	6 Years	Review and if no longer needed destroy	Includes minor meetings/projects and departmental business meetings
Destruction Certificates or Electronic Metadata destruction stub or record of information held on destroyed physical media	Destruction of record or information	20 Years	Consider Transfer to a Place of Deposit and if no longer needed to destroy	The Public Records Act 1958 limits the holding of records to 20 years unless there is an instrument issued by the Minister with responsibility for administering the Act. If records are not excluded by such an instrument they must either be transferred to a Place of Deposit as a public record or destroyed 20 years after the record has been closed.
Incidents (serious)	Date of incident	20 Years	Review and consider transfer to a Place of Deposit	Incidents (serious)
Incidents (not serious)	Date of incident	10 Years	Review and if no longer needed	
Non-Clinical Quality	End of year to	12 years	Review and if no	

Assurance Records	which the assurance relates		longer needed destroy	
Patient Advice and Liaison Service (PALS) records	Close of financial year	10 years	Review and if no longer needed destroy	
Policies, strategies and operating procedures including business plans	Creation	Life of organisation plus 6 years	Review and consider transfer to a	

Record Type	Retention start	Retention period	Action at end of retention period	Notes
6. Communications				
Intranet site	Creation	6 years	Review and consider transfer to a Place of Deposit	
Patient information leaflets	End of use	6 years	Review and consider transfer to a Place of Deposit	
Press releases and important internal communications	Release Date	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	End of consultation	5 years	Review and consider transfer to a Place of Deposit	
Website	Creation	6 years	Review and consider transfer to a Place of Deposit	

Record Type	Retention start	Retention period	Action at end of retention period	Notes
7. Staff Records & Occupational Health Although pension information is routinely retained until 100th birthday by the NHS Pensions Agency employers must retain a portion of the staff record until the 75th birthday.				
Duty Roster	Close of financial year	6 years	Review and if no longer needed destroy	
Exposure Monitoring information	Monitoring ceases	40 years/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 other case, for at least 5 years.
Occupational Health Reports	Staff member leaves	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	Staff member leaves	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	Staff member leaves	50 years from the date of the last entry or until 75th birthday, whichever is longer	Review and if no longer needed destroy	Occupational Health Report of Staff member under health surveillance where they have been subject to radiation doses
Staff Record	Staff member leaves	Keep until 75thbirthday (see Notes)	Create Staff Record Summary then review or destroy the main file	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. May be destroyed 6 years after the staff member leaves or the 75th birthday, whichever is sooner, if a summary has been made.
Staff Record Summary	6 years after the staff member leaves	75thBirthday	Place of Deposit should be offered for continued retention or Destroy	Please see the good practice box Staff Record Summary used by an organisation.

Record Type	Retention start	Retention period	Action at end of retention period	Notes
Timesheets (original record)	Creation	2 years	Review and if no longer needed destroy	
Staff Training records	Creation	See Notes	Review and consider transfer to a Place of Deposit	Records of significant training must be kept until 75thbirthday 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 IGA recommends: • Clinical training records - to be retained until 75thbirthday 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 completed • Other training records - keep for six years after training completed

Record Type	Retention start	Retention period	Action at end of retention period	Notes
8. Procurement				
Contracts sealed or unsealed	End of contract	6 years	Review and if no longer needed destroy	
Contracts - financial approval files	End of contract	15 years	Review and if no longer needed destroy	
Contracts - financial approved suppliers documentation	When supplier finishes work	11 years	Review and if no longer needed destroy	
Tenders (successful)	End of contract	6 years	Review and if no longer needed destroy	
Tenders (unsuccessful)	Award of tender	6 years	Review and if no longer needed destroy	

Record Type	Retention start	Retention period	Action at end of retention period	Notes
9. Estates				
Building plans and records of major building work	Completion of work	Lifetime of the building or disposal of asset plus six years	Review and consider transfer to a Place of deposit	Building plans and records of works are potentially of historical interest and where possible be kept and transferred to a place of deposit
CCTV		See ICO Code of Practice	Review and if no longer needed destroy	ICO Code of Practice: https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf The length of retention must be determined by the purpose for which the CCTV has been deployed. The recorded images will only be retained long enough for any incident to come to light (e.g. for a theft to be noticed) and the incident to be investigated.
Equipment monitoring and testing and maintenance work where asbestos is a factor	Completion of monitoring or test	40 years	Review and if no longer needed destroy	
Equipment monitoring and testing and maintenance work	Completion of monitoring or test	10 years	Review and if no longer needed destroy	Equipment monitoring and testing and maintenance work
Inspection reports	End of lifetime of installation	Lifetime of installation	Review	Inspection reports
Leases	Termination of lease	12 years	Review and if no Longer needed destroy	Leases
Record Type	Retention start	Retention period	Action at end of retention period	Notes
Minor building works	Completion of work	retain for 6 years	Review and if no longer needed destroy	Minor building works
Photographic collections of service locations and events and activities	Close of collection	Retain for not more than 20 years	Consider transfer to a place of deposit	The main reason for maintaining photographic collections is for historical legacy of the running and operation of an organisation. However, photographs may have subsidiary uses for legal enquiries.
Radioactive Waste	Creation	30 years	Review and if no longer needed destroy	

Sterilix Endoscopic Disinfector Daily Water Cycle Test, Purge Test, Ninhydrin Test	Date of test	11 years	Review and if no longer needed destroy	
Surveys	End of lifetime of installation or building	Lifetime of installation or building	Review and consider transfer to Place of deposit	

Record Type	Retention start	Retention period	Action at end of retention period	Notes
10. Finance				
Accounts	Close of financial year	3 years	Review and if no longer needed destroy	Includes all associated documentation and records for the purpose of audit as agreed by auditors
Benefactions	End of financial year	8 years	Review and consider transfer to Place of Deposit	These may already be in the financial accounts and may be captured in other records/reports or committee papers. For benefactions, endowment, trust fund/legacies, offer to a Place of Deposit.
Debtor records cleared	Close of financial year	2 years	Review and if no longer needed destroy	Debtor records cleared
Debtor records not cleared	Close of financial year	6 years	Review and if no longer needed destroy	Debtor records not cleared
Donations	Close of financial year	6 years	Review and if no longer needed destroy	Donations
Expenses	Close of financial year	6 years	Review and if no longer needed destroy	Expenses
Final annual accounts report	Creation	Before 20 years	Transfer to place of deposit if not transferred with the board papers	Should be transferred to a place of deposit as soon as practically possible

Financial records of transactions	End of financial year	6 Years	Review and if no longer needed destroy	
Petty cash	End of financial year	2 Years	Review and if no longer needed destroy	
Private Finance initiative (PFI) files	End of PFI	Lifetime of PFI	Review and consider transfer to Place of Deposit	
Salaries paid to staff	Close of financial year	10 Years	Review and if no longer needed destroy	Salaries paid to staff
Superannuation records	Close of financial year	10 Years	Review and if no longer needed destroy	

Record Type	**Retention start**	**Retention period**	**Action at end of retention period**	**Notes**
11. Legal, Complaints & Information Rights				
Complaints case file	Closure of incident (see Notes)	10 years	Review and if no longer needed destroy	http://www.nationalarchives.gov.uk/documents/information-management/sched_complaints.pdf The incident is not closed until all subsequent processes have ceased including litigation. The file must not be kept on the
Fraud case files	Case closure	6 years	Review and if no longer needed destroy	
Freedom of Information (FOI) requests and responses and any associated correspondence	Closure of FOI request	3 years	Review and if no longer needed destroy	Where redactions have been made it is important to keep a copy of the redacted disclosed documents or if not practical to keep a summary of the redactions.
FOI requests where there has been a subsequent appeal	Closure of appeal	6 years	Review and if no longer needed	

Industrial relations including tribunal case records	Close of financial year	10 Years	Review and consider transfer to a Place of Deposit	Some organisations may record these as part of the staff record but in most cases they will form a distinct separate record either held by the staff member/manager or by the payroll team for processing.
Litigation records	Closure of case	10 years	Review and consider transfer to a Place of Deposit	
Patents / trademarks / copyright / intellectual property-	End of lifetime of patent or termination of licence/ action	Lifetime of patent or 6 years from end of licence/ action	Review and consider transfer to Place of Deposit	
Software licences	End of lifetime of software	Lifetime of software	Review and if no longer needed destroy	
Subject Access Request (SAR) and disclosure correspondence	Closure of SAR	3 Years	Review and if no longer needed destroy	
Subject Access Request where there has been a subsequent appeal	Closure of appeal	6 Years	Review and if no longer needed destroy	

Information Governance Alliance - Records Management Code of Practice for Health and Social Care 2016

Equality and Human Rights Analysis

Title: Corporate Records Policies
Area covered: Trustwide

What are the intended outcomes of this work? To give guidance on the creation, storage and management of Corporate Records to ensure the Trust meets its obligations in relation to Information Governance and Records Management.
Who will be affected? All staff

Evidence
What evidence have you considered? At review no changes noted.
Disability (including learning disability) Document states that it is available in different formats available on request by the author.
Sex At review no changes noted
Race At review no changes noted
Age At review no changes noted
Gender reassignment (including transgender) At review no changes noted
Sexual orientation At review no changes noted
Religion or belief At review no changes noted
Pregnancy and maternity At review no changes noted
Carers At review no changes noted
Other identified groups At review no changes noted
Cross Cutting At review no changes noted

Human Rights	Is there an impact? How this right could be protected?
Right to life (Article 2)	*not engaged at review*
Right of freedom from inhuman and degrading treatment (Article 3)	*Use supportive of a HRBA*
Right to liberty (Article 5)	Not engaged at review
Right to a fair trial (Article 6)	Not engaged at review
Right to private and family life (Article 8)	Not engaged at review
Right of freedom of religion or belief (Article 9)	Not engaged at review
Right to freedom of expression Note: this does not include insulting language such as racism (Article 10)	Not engaged at review
Right freedom from discrimination (Article 14)	Not engaged at review

Engagement and Involvement
This policy has gone through Equality & Human Rights process.

Summary of Analysis

Eliminate discrimination, harassment and victimisation

This policy has gone through Equality & Human Rights process.

Advance equality of opportunity

To ensure it does not directly or indirectly discriminate

Promote good relations between groups

To support the Trust to meet its Equality Act duties

What is the overall impact?

There has been no equality or human rights issues identified within the document.

Addressing the impact on equalities

Not required

Action planning for improvement

No actions noted.

For the record

Name of persons who carried out this assessment:

Kate Greenwood **Gina Kelly reviewed document**
Jacquie Ruddick **Gina Kelly reviewed document**
Gina Kelly **Geoff Springer reviewed**

Date assessment completed:

19 October 2011 **Reviewed 20 January 2016** **Reviewed 7 September 2017**
Reviewed 28th May 2019 Reviewed 30th April 2020

Name of responsible Director:

Director of IPI

Date assessment was signed:

19/10/2011 **12/09/2017**