University Hospitals of Leicester NHS
NHS Trust

Corporate Records Management Policy

Approved By:	Policy & Guideline Committee
Date of Original Approval:	19 June 2020
Trust Reference:	B25/2020
Version:	3
Supersedes:	2 – January 2022 Policy and Guideline Committee
Trust Lead:	Saiful Choudhury - Head of Privacy
Board Director Lead:	Andrew Carruthers – Chief Information Officer & Senior Information Risk Owner
Date of Latest Approval	20 December 2023 – PGC Chair's urgent approvals process
Next Review Date:	May 2025

CONTENTS

REVIEW DATES AND DETAILS OF CHANGES MADE DURING THE REVIEW

VERSION	DATE	AUTHOR	CHANGE
V2	DEC 2023	SC	Link to Record retention schedule updated
V2	NOV 2021	SC	Links updated. Gramatical changes. Roles and responsibilities updated along with telephone numbers.

KEY WORDS

Information Governance, Records, Personal Data

1 INTRODUCTION AND OVERVIEW

1.1 This document sets out the University Hospitals of Leicester (UHL) NHS Trusts Policy and Procedures for Corporate Records Management and Retention within the Trust and need for chairs of groups/meetings to clarify the expectations around maintaining and storing minutes/papers at sub-Executive Board level. Throughout this policy the term “records” should be taken to mean “corporate records”.

1.2 Corporate Records Management is the process by which an organisation manages all the aspects of information 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.

1.3 The Corporate Records Management: NHS Code of Practice has been published by the Department of Health as a guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England. It is based on current legal requirements and professional best practice.

1.4 The Trust's records are its corporate memory, providing evidence of actions and decisions and representing a vital asset to support daily functions and operations. Corporate 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.

1.5 The Trust has adopted this policy and is committed to ongoing improvement of its corporate records management functions as it believes that it will gain a number of organisational benefits from so doing. These include:

- Better use of physical and server space
- Better use of staff time
- Improved control of valuable information resources
- Compliance with legislation and standards
- Reduced costs

1.6 The Trust also believes that its internal management processes will be improved by the greater availability of information that will accrue by the recognition of records management as a designated corporate function.

1.7 As well as applying to all staff this document sets out a framework within which the staff responsible for managing the Trust's records can develop specific policies and procedures to ensure that records are managed and controlled effectively, and at best value, commensurate with legal, operational and information needs.

2 POLICY SCOPE

2.1 This policy applies to all Trust staff and relates to all non-clinical records held in any format by the Trust. These are:

- **All administrative records** (e.g. personnel, estates, financial and accounting records, agendas, minutes, duty rosters, audits, notes associated with complaints).

2.2 The required retention periods for documents is retained within a retention schedule that details the **Minimum Retention Period** for each type of corporate record. Records (whatever the media) may be retained for longer than the minimum period. However, records should not ordinarily be retained for more than 30 years. Where a period longer than 30 years is required (e.g. to be preserved for historical purposes), or for pre 1948 records, contact the Privacy Unit who will discuss transfer of the information to the local Records Office.

2.3 The key components of corporate records management policy are:

- Record creation

- Record retrieval
- Record security and storage
- Record maintenance (including tracking of record movements)
- Tracking and transportation
- Disposal and destruction

For ease of reference this policy is supported by a number of procedures which must be followed when undertaking the activity described above.

Where independent specialty areas develop additional local procedures then they must fully comply with the requirements of this policy and its supporting procedures.

3 DEFINITIONS AND ABBREVIATIONS

3.1 ***Corporate Records*** are 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.

3.2 **Data Security & Protection Toolkit (DS&P Toolkit);** The Data Security & Protection Toolkit is an online self-assessment tool that allows organisations to measure their performance against the National Data Guardian's 10 data security standards. All orgnanisations that have access to NHS patient data and systems must use this toolkit to provide assurance that they are practising good data security and that personal information is handled correctly.

3.3 A ***Document*** is any piece of written information in any form, produced or received by an organisation or person. It can include databases, website, email messages, word and excel files, letters, and memos. Some of these documents will be ephemeral or of very short-term value and should never end up in a records management system (such as copies circulated for information only, publications available elsewhere or All staff announcements). This includes written information sent by texts and/or posted on social media platforms e.g. Twitter / WhatsApp

Some documents will need to be kept as evidence of business transactions, routine activities or as a result of legal obligations, such as policy documents. These should be placed into an official filing system and at this point, they become official records. In other words, all records start off as documents, but not all documents will ultimately become records.

3.4 A ***File Plan*** is a document that lists the records held within the organisation and describes the type of records, the location where they should be stored, the rules applying to them, the retentions associated to them and the person or persons responsible for their management.

3.5 ***Personal data*** is defined as data relating to a living individual that enables him/her to be identified either from that data alone or from that data in

conjunction with other information in the data controller's possession. It therefore includes such items of information as an individual's name, address, age, race, religion, gender and physical, mental or sexual health.

3.6 In this policy, ***Records*** are defined as 'recorded information, in any form, created or received and maintained by the Trust in the transaction of its business or conduct of affairs and kept as evidence of such activity'.

3.7 The term ***Records Life Cycle*** 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

3.8 ***Transitory records*** are records that have only temporary value. They are produced in the completion of routine actions, in the preparation of other records that supersede them and / or for convenience of reference. They are NOT official copies of records which need to be retained as evidence of an activity and they have no significant informational value after they have served their primary purpose. Examples of transitory records are working documents – drafts or rough notes, preliminary versions and supporting information required to create final documents.

4 ROLES

Responsibilities within the Organisation

4.1 **Executive Lead for Records:** The Executive Lead has overall responsibility for records management in the Trust. As Accountable officer he/she is responsible for the management of records within the Trust and for ensuring appropriate mechanisms are in place to support service delivery and continuity. 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. The Executive Lead for Records is the Chief Information Officer

4.2 **Senior Information Risk Owner (SIRO):** The SIRO is a nominated person (Executive or Senior Manager on the Executive IM&T Board) who is familiar with information risk and the organisations response to risk. The SIRO takes ownership of the organisation's information risk policy and acts as an advocate for information risk on the Executive IM&T Board. The SIRO for the Trust is the Chief Information Officer for IM&T.

4.3 **Caldicott Guardian:** The Trust's Caldicott Guardian has a particular responsibility for reflecting patients' interests regarding the use of patient identifiable information. They are responsible for ensuring patient identifiable information is shared in an appropriate and secure manner. The Caldicott Guardian for the Trust is the Medical Director.

4.4 **Information Governance Steering Group:** The Information Governance Steering Group (IGSG) is responsible for ensuring that this policy is implemented and maintaining oversight of records management compliance against national requirements e.g.

- Care Quality Commission requirements

- Data Security & Protection Toolkit.

4.5 **Head of Privacy (Data Protection Officer):** The Head of Privacy & Information Risk is responsible for ensuring the corporate record elements of this policy are implemented, facilitating compliance of corporate records and maintaining a performance management framework. The Head of Privacy & Information Risk also has lead responsibility for Data Protection, Confidentiality and the Data Security & Protection Toolkit within the Trust. Ensuring staff have access to the up to date guidance on keeping personal information secure; ensuring that evidence is made available to support the attainment levels reported to Connecting for Health; reviewing and evaluating IG arrangements and communicating changes in assessment/guidance across all functional areas; The Head of Privacy should be contacted in the event of IG queries or incidents.

4.6 **Managers within CMGs / Directorates:** The responsibility for local records management is devolved to the relevant directors, clinical management group managers, directorate managers and department managers. Heads of Departments, other units and business functions within the Trust have overall responsibility for the management of records generated by their activities, i.e. for ensuring that records controlled within their unit are managed in a way which meets the aims of the Trust's records management policies.

4.7 **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.

5. POLICY IMPLEMENTATION AND ASSOCIATED DOCUMENTS

5.1 Legal and Professional Obligations

All NHS records are Public Records under the Public Records Acts. The Senior Information Risk Owner (Chief Information Officer) will take actions as necessary to comply with the legal and professional obligations set out in the Records Management: NHS Code of Practice, in particular:

- The Public Records Act 1958
- The Data Protection Act 2018
- The Freedom of Information Act 2000
- The Common Law Duty of Confidentiality
- The NHS Confidentiality Code of Practice
- International Standard ISO 15489, Records Management

and any new legislation affecting records management as it arises.

5.2 Policy Statement

5.2.1 When Trust staff manage a Record then they are required to comply with the requirements of the Procedures and Requirements which appear as Appendices to this Policy.

5.2.2 The Privacy Unit will establish and maintain mechanisms through which departments and other units can register the records they are maintaining. The inventory of record collections will facilitate:

- The classification of records into types
- The recording of the responsibility of individuals creating records.

5.2.3 In Principle – where minutes are created for the purpose of record keeping of meetings at Sub-Executive Board level - there will be the expectation that these minutes will be:

- Validated for Accuracy at the next available meeting and then filed.
- Clearly documented location for where these minutes will be kept/ for how long and at what point they are to be destroyed (if appropriate).

This is to be communicated to the Executive Board at the first meeting of the series/or at earliest opportunity (whichever is first) to establish the record keeping process.

5.3 **Retention and Disposal Schedules**

5.3.1 It is a fundamental requirement that all of the Trust's records are retained for a 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.

5.3.2 The Trust has adopted the retention periods obtained from the NHS corporate retention schedule. This can be found here, or by simply searching 'NHS corporate retention schedule' on the internet.

6 EDUCATION AND TRAINING REQUIREMENTS

All staff are required to undertake mandatory annual Cyber Security training through the UHL training system as defined within the UHL Core Statutory and Mandatory Training Policy.

Given the variety of records within the organisation, which will be clinical, non clinical, electronic or manual, identifying additional training needs and training provision is the responsibility of local records managers and electronic systems owners.

All managers must ensure that their staff receive the appropriate training for the corporate records which they keep (e.g. staff files) or the record systems where dealing with staff data.

7 PROCESS FOR MONITORING COMPLIANCE

7.1 Specific monitoring criteria are detailed in each of the appendices of this policy.

POLICY MONITORING TABLE

The top row of the table provides information and descriptors and is to be removed in the final version of the document

Element to be monitored	Lead	Tool	Frequency	Reporting arrangements Who or what committee will the completed report go to.
File plan – All Record entries will have attributes recorded	Head of Privacy	Sampling data (randomised) via Spreadsheet (3 records)	Yearly	The Audit results will be reported to the Information Governance Steering Group (IGSG).
File plan – Attributes will reflect accurate information	Head of Privacy	A sample of 3 record entries from each CMG / corporate area will be checked that the attributes detailed are recorded accurately i.e. records can be found in the locations recorded.	Yearly	The Audit results will be reported to the Information Governance Steering Group (IGSG).

8 EQUALITY IMPACT ASSESSMENT

8.1 The Trust recognises the diversity of the local community it serves. Our aim therefore is to provide a safe environment free from discrimination and treat all individuals fairly with dignity and appropriately according to their needs.

8.2 As part of its development, this policy and its impact on equality have been reviewed and no detriment was identified.

9 SUPPORTING REFERENCES, EVIDENCE BASE AND RELATED POLICIES

There are a number of policies and procedures within the Trust that should be read inconjunction with this document for a complete understanding of how the Trust is organised and the strategies in place to fulfil its obligations. The key documents are listed below:

- Data Protection Policy A6/2003
- Information Governance Policy B4/2004
- E-mail and Internet Access and Monitoring Policy A9/2003
- Information Security Policy A10/2003
- Freedom of Information Act 2000
- Environmental Information Regulations 2005
- Agile Working (including Home Working) Policy and Procedure

10 PROCESS FOR VERSION CONTROL, DOCUMENT ARCHIVING AND REVIEW

The updated version of the Policy will then be uploaded and available through INsite Documents and the Trust's externally-accessible Freedom of Information publication scheme. It will be archived through the Trusts PAGL system

Appendix A – Corporate Records Management Procedure

Corporate Records Management Procedure	University Hospitals of Leicester NHS NHS Trust

A1 Introduction

The following documents the procedures for ensuring that corporate electronic and paper records are accessible and retrievable when and where required. It is not only concerned with corporate records that are part of a formal electronic document but includes records on network drives and in shared folders. It also includes emails and attachments, along with web pages on Internet and Intranet sites that are considered corporate records.

A2 Paper Records Management Procedures

It is a requirement of both the Department of Health's Data Protection & Security Toolkit and UHL's Corporate Records Management Policy to have in place, appropriate procedures to support records creation, maintenance, storage, retrieval and file deletion. While many of the Trust's corporate records are created and held in electronic form, there remains a requirement to have procedures for the good management of paper records.

Corporate records are created to ensure that the Trust has adequate information to deliver high quality services and provide evidence of their activities.

A2.1 Creation of Paper Records

All records should be identified clearly on the file cover with:

- An accurate title and description and where appropriate
- The department/service
- Name of relevant member of staff

Records and documents may be classified into several categories, e.g. draft, confidential, sensitive, restricted or unrestricted. If a protective mark is required for a particular record, ensure that each record is consistently added to the correct local category.

Documents within a file should be securely fastened. It is advised that plastic wallets and files with pockets/flaps should not be used as loose papers can easily be lost from them.

A2.2 Paper Record Naming

Where possible staff are expected to follow advice issued by The National Archives, i.e.

- Give a unique name to each recordGive 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)

A2.3 Records Maintenance

Papers contained within the file should be arranged in a logical structure and be ordered chronologically. Where not required duplicate copies should be removed and where a file becomes too large, a second volume should be created. The original should be kept in safe and be accessible if necessary.

A2.4 Amendments to Records

Any amendments made retrospectively to a record must clearly indicate that the additional entry was made as an addition to the earlier record. At no point should an attempt be made to alter or delete the earlier record.

A2.5 Tracking and Tracing Paper Records

Where multiple person access and removal/transfer of records from their usual storage locations exist each department should keep a simple log of records removed, this will ensure that the movement and location of records is controlled and provides an auditable trail of record transactions. This could be done either in book form, manual tracer card or electronically e.g. as an Excel Spreadsheet. The tracking and tracing log should document the following items:-

- File Reference
- File Name
- Date Accessed or Removed
- Name of Person Accessing or Removing Record
- Contact Details for Individual Gaining Access or Removing Record
- Location Removed to (if Applicable)
- Date returned (If applicable)

A2.6 Missing/Mislaid Records Procedure

It is the responsibility of all staff to minimise the risk of mislaid or missing records through effective control of their location and

movement. This procedure must be followed in all instances of mislaid or missing records.

Definitions:

- Records are classified as being mislaid when they cannot be found following a search of the relevant area. This would include a check of the file tracking/tracing system
- Records are classified as missing if not located after a period of 3 working days
- In the first instance the potential data loss should be notified to the Head of Privacy
- Incidents are reported through Datix the Trust's incident reporting system

A2.6.1 Mislaid Records

Where a record cannot be located after the initial search the following procedure should be carried out:

- Report the incident to the line manager who will take responsibility for the investigation and advise the Head of Privacy;
- Flag the incident on any relevant computer system and/or on the file tracer card where applicable;
- The line manager will ensure a thorough search is undertaken of the relevant and surrounding areas as appropriate;
- Where appropriate the line manager, as part of the investigation will widen the search to include other locations and departments.

A2.6.2 Missing Records

Where a record has not been located after 3 days, the following procedure should be carried out:

- The record will be flagged as 'missing' on any relevant computer system and/or file tracer card;
- Where applicable a new set of records should be created, marked 'Duplicate set' and dated, if the record is in current use;
- It may be necessary to inform the patient/service user. This should be discussed between the relevant health/social care professional and the records management lead/line manager where appropriate;

- The line manager will report the incident (Datix incident reporting system) in line with incident reporting policies and will inform the Head of Privacy.

A2.6.3 Found Records

Where a missing record is subsequently found, the following procedure should be carried out:

- The duplicate set of records must be merged;
- The relevant computer systems and/or the file tracer card must be updated;
- The Risk & Assurance Manager and the Head of Privacy must be advised;
- If the patient/service user has been notified that their record is missing then they should be advised if it is found;
- Datix should be updated to reflect that the record has been found.

A2.7 Retention and Disposal of Paper Records

Corporate records should be retained in accordance with National Guidance found here: Records Management Code of Practice - NHS Transformation Directorate (england.nhs.uk)
Where records become inactive but still need to be retained arrangements should be made for their transport to a suitable secure area within the Trust or alternative storage e.g. offsite storageRecords should not be allowed to accumulate in offices where they might pose a health and safety risk and also take up space that could be put to better use.

In some cases records may be scanned into an electronic format for further archiving or deemed as being historically significant and transferred to an archive for permanent preservation.

Arrangements should be made for the secure destruction of any confidential paper records.

A2.8 Offsite Storage of Paper Records

When using offsite storage the following criteria must be adhered to:

- There must be a service level agreement (SLA) which details the nature and level of service to be provided. It should include the cataloguing of requests, destruction arrangements and timescales for retrieval. This must be signed by both parties and retained.
- A catalogue of records and their destruction dates must be kept (this may be provided by the storage company by arrangement);
- Invoices must not contain personal identifiable information.

A2.9 Evidential Value of Scanned Documents

Definition: Evidential records - records which are necessary to provide an authentic and adequate evidence of the Trust's actions, functions, policies, and/or structure. Evidential value relates to the document's creation and not necessarily to its content.

Before a decision is made to scan a record type into an electronic medium and destroy the original, consideration must be made regarding:

- The cost of scanning compared with the cost of retaining the records in original format e.g. reduced storage requirements and business efficiency;
- Whether the records are of any archival value and there needs to be consultation prior to destruction;
- Format of preservation: scanned records must be retrievable should there be an improvement in information technology. Microfiche should not be used in case there is a need to provide good quality copies in defence of a complaint or a claim; and
- The need to protect the evidential value of the original unscanned record.

Further advice on scanning can be sought from the Head of Privacy ext

6053

A2.9.1 What to Scan

Records requiring a long term or permanent retention in accordance with the Access to Health Records 1990 guidance from NHS Digital Retention Schedule should be considered for scanning to ensure that the need for storage space for paper records is kept to a minimum.

A2.10 Records Which Should Not Be Destroyed

Records should only be destroyed in accordance with the Trust Retention of Records Policy. Additionally in the case of an ongoing complaint, Freedom of Information Act request, Data Protection Act request or legal claim anticipated, the original documents should not be destroyed. Similarly if a claim is ongoing the original records should be retained and there is usually a standard direction from a Court at the first Case Management Hearing to that effect.

Where records are identified to be kept for longer than the guidelines for retention (i.e. in the case of a complaint, litigation etc) it is the responsibility of the department concerned to raise a flag on any relevant systems and clearly mark the original records to highlight this.

A3 Electronic Records Management Procedures

Electronic documents must be managed to the same standards expected of paper records.

A3.1 Aim of the Procedure

The aim of this procedure is to ensure that:

- 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.

A3.2 Electronic Records – Actions

This procedure sets out the actions that must be undertaken in order to ensure that all electronic records:

- Provide audit trails to accurately log when records are created, accessed, amended or disposed of appropriately;
- 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;
- Are controlled with regards to access to records through a variety of security measures, including user verification, password protection and access monitoring where appropriate;
- Will remain accessible and usable throughout their life cycle;
- Can be cross-referenced with their paper counterparts (where dual systems are maintained) and can be relied upon to have evidential value should there be a need to rely on them following an incident, complaint or litigation.

A3.3 Creation of Electronic Records

When creating a record you need to decide on the most appropriate format (e.g. paper/electronic) for it. This decision should be based on what the record is to be used for. For example there are occasions when the most appropriate format for a record is paper, perhaps because the record needs to be signed. On many occasions the most appropriate format is an electronic format.

A3.4 Referencing

The corporate areas of the Trust should use a referencing system that meets its business needs, and can be easily understood by staff members that create electronic documents and 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. 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.

A3.5 Electronic Record Naming

'File names' are the names that are listed in the computers file directory that users give to new files when they save them for the first time. Naming records consistently, logically and in a predictable way will distinguish similar records from one another at a glance, and by doing so will facilitate the storage and retrieval of records, which will enable users to browse file names more effectively and efficiently. Naming records according to an agreed convention should also make file naming easier for colleagues because they will not have to ‘re-think’ the process each time.

Where documents are stored on network drives keep file names short, but meaningful:

- Avoid unnecessary repetition and redundancy in file names and file paths;
- Use capital letters to delimit words i.e. **R**ecords**M**inutes**N**ov20111101, **not** spaces or underscores;
- When including a number in a file name always give it as a two-digit number, i.e. 01-99, unless it is a year or another number with more than two digits;
- If using a date in the file name always state the date ‘back to front’, and use four digit years, two digit months and two digit days, e.g.YYYYMMDD;
- When including a personal name in a file name give the family name first followed by the initials;
- Avoid using common words such as ‘draft’ or ‘letter’ at the start of file names, unless doing so will make it easier to retrieve the record;
- Order the elements in a file name in the most appropriate way to retrieve the record;
- The file names of records relating to recurring events should include the date and a description of the event, except where the inclusion of any of either of these elements would be incompatible with the second point;

The file names of correspondence should include the name of the correspondent, an indication of the subject, the date of the correspondence and whether it is incoming or outgoing correspondence,

except where the inclusion of any of these elements would be incompatible with the second point.

A3.6 Version Control – Electronic Records

Definition: '*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 a number of different users, and those changes may not be immediately apparent. Version control is also important when working on a collaborative document with a number of contributors and/or frequent revisions, for example a consultation response.
- Use a unique version number to distinguish one version from another.
- Use this procedure for all documents where more than one version exists, or is likely to exist in the future.
- Use a version numbering system that uses version numbers with points to reflect major and minor changes, such as version 1.1 (first version with minor change), version 2.0 (second version with a major change), version 2.2 (third version with a minor change).
- Put the version number and date on the document itself. Common places for version numbers are the document cover, or in either the header or footer text of each page.
- Working drafts can use v 0.1 as the starting point and continue to 0.2, etc. with additional amendments and comments.

A3.7 Read-only tag

To reduce the likelihood of one version being overwritten with another use the read- only tag where appropriate.

Applying a read-only tag will prompt users to save the document with a new file name if they make any changes to the original document. This should be used for finalised documents where loss of the original would be a problem.

A3.8 Back up

All electronic records stored on shared or network drives should be routinely backed up. Clinical and IT systems are centrally managed and backed up via IM&T.

Colleagues requiring storage will be expected to either contact their line manager to request access to a sharepoint location to save work (such as research/audits) or arrange to contact service desk to have a location created for them ensuring that access rights are correctly set to ensure

confidentiality is maintained and material can only be viewed by intended personnel. USB and Hard drives must be procured from the Trust for Trust usage in exceptional cases where there is no internet access available or where sharepoint is not feasible. These requests will be considered by the Privacy Unit on a case by case basis following escalation from service desk.

A3.9 Record Copies / Emails

Emails come within the definition specified in the scope of this guidance and are classed as corporate records in exactly the same way as any other documents.

Copies are to be saved of any email considered to be a record. In order to complete this action satisfactorily the employee should have a suitable process in place to manage their email inbox in order not to overload the organisational and personal mailbox size. Appropriate advice is available through the IT Department. However, staff are not expected to keep a copy of routine emails, e.g. those accepting / declining meetings etc.

The correct management of emails is detailed in the Trust's E-mail and Internet Access and Monitoring Policy A9/2003

A3.10 Retention and Destruction

All electronic records must be retained in accordance with the retention and destruction schedules found here: Records Management Code of Practice - NHS Transformation Directorate (england.nhs.uk)

A4 File Plan

It is the responsibility of the Services and Departments to maintain a file plan to enable the Trust to keep track of the records held and to assist with records auditing and control (see Schedule 1).

The file plan will record all corporate records in paper and electronic form and detail key attributes about the records e.g. locations stored, retention dates etc.

- The information held in paper records and electronic may be required to respond to a request under the Freedom of Information Act 2000. Such requests must be processed within specific time limits which require records to be readily accessible to authorised staff.
- Records should be stored securely and not left unattended or accessible to staff not authorised to see them.
- Where records are removed from the office, a tracking system should record who has removed the file and where it is. The process need not be a complicated one, e.g. a book that staff members sign when a record or file is removed or returned.

- Records should be transported securely.
- Files should be given clear and logical names to assist filing and retrieval of records.
- Filing of corporate records in desk drawers should not occur and must be placed in the appropriate filing system.

A5 Occasional usage at home/Agile working

It is recognised that there are occasions where staff may need to take/access UHL information at home. Appropriate security measures must be adopted to safeguard the information whilst transporting and whilst held within their home.

- Only members of staff are allowed access to information being used at home in any form, on any media.

- Use of any information at home must be for work purposes only

- Staff must ensure the security of the information within their home. Where possible it should be stored in a locked container (filing cabinet, lockable briefcase). If this is not possible, when not in use it should be neatly filed and stored in a way that it is not obvious to other members of the household.

- Staff must ensure their devices (Laptops, Ipads and/or Mobile Devices) are secured with a password which conforms with the Password Policy.

- Any personal/sensitive (inc. patient and staff information) or organisationally confidential information that has to be taken home must be within folders marked 'private and confidential' and other members of the household instructed not to look at it.

A6 Monitoring

The Head of Privacy will undertake a yearly audit of the File Plan to assess the accuracy of the records it lists.

Omissions in the detail will be reported to the responsible lead for the associated area and a sample of 3 record entries from each CMG / corporate area will be checked that the attributes detailed are recorded accurately i.e. records can be found in the locations recorded.

The results will be reported to the Information Governance Steering Group (IGSG).

Appendix B – Retention Schedule

Retention Schedule	University Hospitals of Leicester NHS NHS Trust

Records Management Code of Practice - NHS Transformation Directorate (england.nhs.uk)