PAPER AND ELECTRONIC CORPORATE RECORDS PROCEDURE

The purpose of this Procedural Guideline document is to ensure that the Trust efficiently and effectively manages the creation, filing, retrieval, appraisal, archive and destruction of electronic and paper corporate records.

The Trust monitors the implementation of and compliance with this operational policy in the following ways:

This process is monitored via the Information Governance Toolkit and assurance reports are submitted to the Information Governance Steering Committee.

<table>
<thead>
<tr>
<th>Services</th>
<th>Applicable</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trustwide</td>
<td>✔️</td>
<td></td>
</tr>
</tbody>
</table>

The Director responsible for monitoring and reviewing this policy is Executive Chief Finance Officer.
ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

PAPER AND ELECTRONIC CORPORATE RECORDS

PROCEDURE CONTENTS

1.0  INTRODUCTION

2.0  PURPOSE

3.0  RESPONSIBILITY

4.0  DOCUMENTS AND RECORDS

5.0  FILING PAPER RECORDS

6.0  ACCESS CONTROL TO THE LASERFICHE SYSTEM

7.0  FILING ELECTRONIC RECORDS

8.0  PRESERVATION OF RECORDS

9.0  DOCUMENT SCANNING

10.0  ELECTRONIC RECORD RETRIEVAL

11.0  ELECTRONIC RECORD DISPOSAL

12.0  REFERENCE TO OTHER POLICIES AND PROCEDURES

APPENDICES

APPENDIX A- QUALITY ASSURANCE FORMS

APPENDIX B- NOTICES (PHOTOCOPIES/TORN/DAMAGED DOCUMENTS)

APPENDIX C- DO’S AND DON’TS FOR PAPER FILING PRACTICES

APPENDIX D- DO’S AND DON’TS FOR ELECTRONIC FILING PRACTICES
PAPER AND ELECTRONIC CORPORATE RECORDS
(LASERFICHE) PROCEDURE

Assurance Statement

The purpose of these procedure guidelines is to ensure that the Trust efficiently and effectively manages the creation, filing, retrieval, appraisal, archive and destruction of electronic and paper corporate records. These guidelines are implemented in adherence to the NHS Connecting for Health Information Governance Toolkit Requirement 601 “Documented and implemented procedures are in place for the effective management of corporate records”, as well as in accordance with the Records Management: NHS Code of Practice, and other relevant guidance and legislation and general good practice in records management.

1.0 INTRODUCTION

1.1 Rising costs of archive storage means The Trust has needed to look at alternatives for timely and accurate access to records.

1.2 The Trust has therefore introduced an electronic storage and retrieval system which will underpin its corporate record management strategy for the future.

1.3 There are a number of benefits to be gained from the gradual movement of paper records to electronic records:

- Reduces filing / storage space by the removal of existing filing racks and cabinets freeing up space for other purposes
- Central record of relevant files
- Meets the health and safety and legislative and other storage criteria set for NHS organisations
- Improves Trust wide access to files and documents
- Reduces the incidences of lost / missing files and provides concrete disaster contingency
- Moves the Trust in the direction of full electronic corporate records

2.0 PURPOSE

2.1 The purpose of this procedure is to enable all staff to understand:

- The difference between a document and a record
- Where and how a record should be filed
- The referencing to be applied to new records
- The naming conventions in use in the Trust
- Version control standards
- If appropriate, how to apply a protective mark
3.0 RESPONSIBILITY

3.1 The Director of ITT is responsible for Trust wide and strategic management of records. In addition the Trust has nominated officers (Head of Electronic Systems & Records / Records Manager) responsible for ensuring compliance with Trust policy and for ensuring records are stored and destroyed in line with Trust policy.

3.2 All staff are responsible for the management of records within their area of activity irrespective of media.

4.0 DOCUMENTS AND RECORDS

Definition of a Record:-

4.1 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’.

4.2 These can be primary, management or support activities. They are kept as audit trail evidence of and information about the Trust's functions, decisions, processes, procedures, operations, proper conduct, rights and obligations, transactions or other activities of the organisation.

4.3 Records can exist in any medium and format, both electronic and hard copy, including but not restricted to e-mail messages, word processing and spreadsheet documents, presentations, PDFs, desktop publishing, scanned images, instant messages, audio, video, databases, electronic forms, computer reports, photographs, CAD and maps.

When does a Document become a Record?

4.4 Not all documents and information are designated as records which must be managed according to Trust policy and procedure. A document becomes a record when:
   - It represents evidence of an activity as described above; and
   - It is finalised and becomes part of the Trust's corporate information

4.5 The following documents will almost certainly become records:
   - Action Plans
   - Building/structural work, property maintenance/repairs, engineers inspection reports
   - Business plans/business cases
   - Commissioned Services
   - Committees, Agendas, Minutes and Terms of Reference
   - Communications/public relations communiqués
   - Complaints papers and correspondence
   - Contract and Tendering records
   - COSHH and other Health & Safety records
   - Financial records / papers
   - Industrial Relations documents
   - Information Governance Toolkit Evidence
   - Internal/External Assurances records
• Major events/notable events (e.g. major incidents, including pandemics, or substantial changes in the provision of local healthcare)
• Major projects and plans (e.g. opening of new buildings; healthcare plans/strategies)
• Ministerial submissions and advice
• Minutes of significant meetings (i.e. where significant decisions are made)
• Papers relating to the preparation of legislation
• Performance monitoring
• Personnel records
• Policies and Strategies
• Policy development documents, reports and correspondence
• Procurement records (e.g. contracts)
• Project Initiation documents (e.g. strategy; requirements, PID, sign off, project review)
• Reports
• Research and development papers
• Superannuation records
• Training records

*This list is not exhaustive*....

4.6 It should be noted that drafts should also be treated as formal records when there is a need for proof of process and the capability to show how ideas developed over time and in response to specific events. Once a document becomes a record, it should not be amended and should only be held in the corporate Electronic Document Records Management System (EDRM) system (or a network drive if you do not yet make use of the corporate EDRM) if electronic, or within a managed filing system if paper. All records should also be retained in line with the retention schedules contained in the Information Governance Alliance Records Management Code of Practice 2015.

**When does a document become a record?**

A document becomes a true record when it is saved and could be via any of the following methods:

• when the document has finished being a draft version e.g. becomes version 1.0 as opposed to 0.1
• when the document has been approved as a true record, e.g. draft minutes are signed off
• When a person decides that a document has to be kept, e.g. as evidence
**How should Non-Records be handled?**

4.7 Not all information is an evidential record. Papers should not be filed if not worth filing and documents should not be kept ‘just in case’. Generally speaking, information that is duplicated, printed from electronic sources for facilitative reasons, out-of-date or superseded and kept for reference rather than evidence, can be discarded once business use has finished. Staff should ensure that these are recycled or if appropriate destroyed as confidential waste. Examples include:

- Junk mail
- Copies of master records
- Drafts printed for proof-reading
- Old forms
- Stationery
- ‘With compliments’ slips (unless used to convey information)
- Catalogues and trade journals
- Non-acceptance of invitations / invitations for events in the past
- Trivial electronic mail messages or notes that are not related to Trust business
- Requests for routine information
- Out-of-date distribution lists

*This list is not exhaustive….*

**Definition of a missing record:**

A ‘*misplaced*’ record is a record that either cannot be found or is unavailable within 5 working days following the first attempt to access that record when required for an out-patient appointment, admission, other patient contact, or for a serious incident.

A record is considered ‘*missing*’ (internally only) when the original file has not been located following all investigations, as detailed in these procedures.

A record is not considered as being ‘*lost*’ e.g. notifiable to the patient (if applicable) until a period of six months has elapsed from the time the record was considered internally ‘missing’ or when time has elapsed for Data Protection Act, Access to Records, FOI requests etc. requests.

A ‘*stolen*’ record describes the physical theft of health record/s from the Trust

Refer to the Misplaced Records Procedure CPG9e
5.0 FILING PAPER RECORDS

Filing Original Paper Records:-

5.1 Please note that this procedure only applies to original paper records. This means evidential records that are received in paper format or are records because they have been stamped, sealed, signed or otherwise annotated. Paper documents that are purely photocopied or printed duplicates are not original records. Place only the master copy of a record on file. Extra copies can be made when necessary. Weed out and destroy low-value, non-record information rather than filing it.

5.2 Always consider whether a paper filing system is really needed. Always try to file documents electronically, unless for practical or legal reasons there is the need to maintain paper files. The Trust provides a support facility for the EDRM system to support all users using the electronic document records management system.

Paper Filing Practices:-

5.3 Fundamentally, paper records should be filed in a secure and environmentally safe filing system, which makes best use of space and meets Health & Safety requirements. Ideally each Department should have a central, shared paper filing system in place.

5.4 Files themselves should be 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. transfer to an archival institution or destruction.

5.5 It is important to arrange files so as not to have conflicting retentions within them and so that security considerations are addressed. For example, this is relevant for Data Protection legislation, as it requires the protection and prompt disposal of personal data. You should therefore establish separate files or file parts for record types with different retention periods and/or confidential information.

(Refer to Appendix C for further guidance on the do’s and don’ts for paper filing practices.)

File Register and Cover Sheet:-

5.6 The existence of all files containing original records must be recorded in a log/register. This register must be used to track the creation, borrowing, movement, archiving or transfer of files, as well as their ultimate disposal. It must allocate a unique identifier (number or alphabetical prefix) to each item / file.
5.7 The file register must be electronic, for example in the use of a spreadsheet or database. The register would contain details such as:

- Department/Team
- File ID
- File Title
- Volume Number
- Room/cabinet location
- Date file opened
- Security constraints on file access
- Date of file closure
- Name and contact details of borrower
- Dates borrowed, expected date for return
- Reason from removing the file
- Special instructions on return (i.e. forward to another source)
- Date file returned
- Date of file closure
- Date and location of archive to a non-office storage location, with any archive box number
- Disposal review date (based on appropriate rule within the Trust’s retention schedule)
- Disposal Date
- Disposal Action (destroyed or transferred)
- Disposal Authority

This list is not exhaustive....

5.8 In applying retention staff have both the retention period (e.g. 6 years) and the ‘trigger’ for that period to begin. The ‘trigger’ could be the date the document was created, the year end in which the document was created, the expiry or termination of a contract, the completion of a project etc. Staff need to note that some document types are to be preserved indefinitely or transferred to The National Archives / Local Archive. Please consult either the Head of Electronic Systems/Records or Records Manager.

5.9 If a dual electronic and paper filing system is maintained for the same records, then a note should be made of the existence and location of the electronic counterparts.

5.10 Every file will need a cover sheet of key information - this is typically attached to the inside cover. The file cover sheet would have information such as the:

- File reference / ID
- File title/name
- Volume number (with any reference to a continuation volume)
- Filing location/department (For return)
- Protective mark
- File begins date
- File ends date
- Disposal review date (based on appropriate rule within the Trust’s retention schedule)

This list is not exhaustive....
5.11 Closing files regularly is key to ensuring that files remain manageable and damage to the records is less likely; it also facilitates the application of disposal processes. After closure, no new papers should be added to it, and it must only be used for reference. Files should be closed when either:

- The file becomes too bulky (over 4cm / 2inch thick);
- The case / project has been completed;
- Papers have not been added to it for two years;
- The contents of the file span more than five years; or
- If appropriate, at the end of the calendar or financial year.
- Files should only be closed in conjunction with retention & destruction guidance

5.12 When a file is closed, this should be clearly marked on the file cover, a reference to the new file marked on the closed file, and a reference to the closed file marked on the new file. Do not begin a new file with a paper referring to another paper that is not on that file.

**File Disposal:-**

5.13 Based on the information within your File Register, you should periodically review paper files to see which have reached their Disposal Review date.

5.14 Based on the rules within the retention schedules contained in the Information Governance Alliance Records Management NHS Code of Practice 2015, from which this review date is to be calculated, the records will either be destroyed or transferred. Do note that these are recommended minimum retention times from the Department of Health, although where there is a business need, records may be retained for longer periods. Where this is the case the decision must be justifiable. Each department should conduct an annual records review. No records should be destroyed without managerial approval and that there is no need to retain specific records for any ongoing, planned or envisaged litigation, audit, investigation or open Freedom of Information request.

5.15 When undertaking destruction, all records will be disposed of in a manner suitable to their confidentiality and commercial sensitivity. Paper records should be shredded and disposed of as confidential waste. Nothing should ever be left in ordinary rubbish bins, open skips or where it might be vulnerable to casual retrieval. If contractors are used, they should be required to sign confidentiality undertakings and to produce written certification as proof of destruction. The procedures within the CP9 Health Records Management Policy and CP9g Storage, Retention and Destruction of Records Procedure should be followed, where appropriate to corporate records.

5.16 Records selected for archival preservation and no longer in regular use by the Trust should be transferred as soon as possible to an archival institution (The National Archives/Local Archive). Non-active records should be transferred no later than 30 years from creation of the record, as required by the Public Records Act 1958. Records, which are thought to be worthy of permanent
preservation, should be referred to the Head of Electronic Systems/Records or the Records Manager for further review.

6.0 ACCESS CONTROL TO EDRM SYSTEM

6.1 New staff must sign up to and abide by the Trusts security, confidentiality and data protection policies.

6.2 A Network Change Control Form must be completed and signed off by Line Managers authorising access to PC systems and electronic records systems. Emails are now accepted from the line manager.

6.3 Active directory will maintain the users of the EDRM system once the system administrators have activated their account.

7.0 FILING ELECTRONIC RECORDS

Where to file Electronic Records

7.1 Laserfiche is the corporate Electronic Document and Records Management System (EDRMS) in the South of the Trust. It is being used to support non-health business functions.

7.2 Laserfiche allows the set up hierarchies of folders, like Windows, within which scanned and electronically created documents will be stored. Documents will also be ‘indexed’ with metadata to allow their profiling, cross-referencing and accurate retrieval. A search for documents can be made via this index metadata as well as their name and actual contents.

7.3 When using Laserfiche, staff will receive training on filing, finding and editing documents.

All electronic (final) records must be filed in Laserfiche, once work in progress is finished and they are finalised (with no further change permitted). Where beneficial, for example in making use of the system’s imaging, search, workflow and version control capabilities, Laserfiche may be used to support work in progress; filing documents from the moment they are received or created.

7.4 Until such time as staff have access to Laserfiche, or where documents like spreadsheets are subject to regular active change, records may be filed in a logical filing structure on the network drive, using network user accounts, with appropriate security access controls applied. This means using shared drives which are secure areas. Electronic records must not be filed or stored on local drives of PCs and laptops (e.g. C:\, My Documents, My Pictures, etc.) or any other removable devices (e.g. USB devices, CD etc.).
**Electronic Filing Practices:-**

7.5 Paper records can be scanned to Laserfiche and electronically generated records can be saved directly from Word, Excel, Outlook and PowerPoint via the ‘Send to Laserfiche’ facility.

7.6 It is important to arrange folders so as not to have records with conflicting retention periods within them. For example, this is relevant for Data Protection legislation, as it requires the protection and prompt disposal of personal data. Consider having separate folders for these records.

7.7 Keep file names short, but meaningful, using keywords relating to the subject of the document. This includes email, where a descriptive title which accurately reflects the content should be chosen. Limit emails to the one subject. Start a new email if the subject matter changes.

7.8 For documents filed on the network, the Trust requires the use of standard naming conventions, as below. The elements of the name would be used as applicable.

- Code: Any relevant reference code
- Date: YYYYMMDD, YYYYMM, YYYY, YYYY-YYYY
- Type: e.g. Minutes, PID, Letter
- Name: Free text, Max 60, Characters
- Status: DRAFT, FINAL
- Version: v0.1, v1.0, v1.1, v2.0

7.9 Within Laserfiche the version control will be automatic however this can be overridden, by an administrator, where necessary. If staff wish to edit a document, they should use the Laserfiche check out/check in capability - this will lock it to an individual for changes, creating a new version when checking back in. Staff should ensure the addition of a version comment.

*(Please refer to Appendix D for further guidance on the do’s and don’ts for electronic filing practices.)*

**Document Indexing:-**

7.10 Within Laserfiche, store records within a folder and profile them with metadata via an index template. The template might have information such as:

- Reference ID (e.g. for staff, cases, transactions, projects, suppliers, assets etc.)
- Project /Job/Contract Names
- Person Names, including correspondents
- Relevant Addresses
- Dates relating to document receipt, dispatch, approval, expiry etc.
- Document types (e.g. job advert, job application, CV)
- Free text descriptions
- Work Status, if applicable
- Closing of activity, case, project, financial period etc.

*This list is not exhaustive....*
7.11 Documents stored within Laserfiche are assigned indexing field values. This permits their profiling, cross-referencing and retrieval via an index search.

7.12 Index fields are grouped together via templates – a template is typically created for a business activity, comprising the fields that are relevant to this process or file type. Templates are applied to both folders and individually to documents.

7.13 Note that the same field can be used across different templates to enable a wider, cross-system search for related documents.

8.0 PRESERVATION OF RECORDS

8.1 Electronic records are much easier to manage in line with the Information Governance Alliance Records Management Code of Practice 2015. Electronic systems can be set to destroy, follow manual prompting or automatically in line with required timescales. For those documents which require permanent preservation the quality of the records will be much better preserved electronically than the traditional paper record to support specific organisational historical data, research, etc.

9.0 DOCUMENT SCANNING

9.1 For those staff using the EDRM system appropriate scanning equipment needs to be provided.

9.2 Trust Administration Hubs will have a scanning station with the ability for local administration staff to scan from / to. Where identified smaller individual scanners will be installed.

9.3 Once scanned, files will be kept in secure storage until the required quality assurance checks have been completed and validated (see Quality Assurance Form, Appendix A).

9.4 Scanning Procedure

9.4.1 All staff will be fully trained by the system administrators – this will include the preparation of files for scanning practice.

9.4.2 Records will require prepping prior to any scanning process taking place. This means that the following work has to be carried out:

- Removal of any paper clips, staples, etc.
- Removal of any post it notes – where these contain information pertinent to the record they should be place on a blank sheet of paper and scanned individually with this page inserted immediately after the original on which the note was attached.
9.5 Committal

9.5.1 Providing all checks as above have been completed and the scanner is satisfied that the file has been scanned correctly, staff are now in a position to commit / store. Once committed / stored documents cannot be altered or added to. The only exception to this via the administrators who can do limited alterations.

9.6 Quality Assurance

9.6.1 Acceptance

- Where processing has enabled selected removal of images i.e. the blank page delete threshold has been set, check the documents to ensure blank pages have been successfully removed.
- If there is any discrepancy or a problem with the images, as defined below, record the details and complete procedure as detailed below.

9.6.2 Definition of Discrepancies

- Image partially or completely obscured – Image found to have another document attached to it that obscures all or part of one or other of the documents.
- Folded documents – Images with evidence that the original document was folded.
- Partial loss of image – Images with evidence that they have loss data on any paper edge.
- Illegible documents – Images for which the content may be partly or wholly unreadable.

9.6.3 Remedial Action

- In the course of carrying out the defined procedure, should a circumstance as described above occur the following remedial actions would be undertaken.

9.6.4 Image Partially or Completely Obscured

- Where an image is found to have another document attached to it that obscures all or part of one or other of the documents additional documents should be checked using the procedures as described above.
- In the event of discovery of a similar fault or loss of image the entire batch of documents scanned should be re-scanned following the documented procedures for such necessary action.
- In the event of no further recurrence with the extended sample testing the single affected batch or documents should be re-scanned following the documented procedures for such necessary action.
9.6.5 **Folded Documents**

- Images with evidence that the original document was folded may or may not result in loss of data from the final image.
- Acceptance of under 2% of images with no evidential loss will be accepted but recorded.
- Loss of image data through folding of original documents will be verified against quality of original documentation. Where documentation is of low or poor quality due to storage or age deterioration or similar condition, acceptance of minimal loss will be made.
- Where loss of data is not defined as above, the single affected file should be re-scanned following the documented procedures for such necessary action.

9.6.6 **Illegible Documents**

- Images for which the content may be partly or wholly unreadable may have been as a consequence of poor or illegible original documentation.
- Where this has been identified the scanning procedure should ensure the inclusion of a statement declaring the document status or use the acknowledgement of such circumstance by the recording of such circumstances in the appropriate documentation.
- Where documents are identified as possibly subject to improvement through re-scan the single affected file or documents (as appropriate) should be re-scanned following the documented procedures for such necessary action.

---

### 10.0. ELECTRONIC RECORD RETRIEVAL

10.1 Only authorised staff will be provided with access to electronic records, as agreed by the completion of the Network Change Control Form.

10.2 Access controls require the following authorisation for the electronic record systems:

- Laserfiche– via Active Directory

10.3 Exceptions to this for printing requests will be for departments / individuals whose roles may specifically require access to written documentation, for example:

- Legal and Insurance
- Complaints
- Information breach investigations
- Integrated Risk
- PPI
- Freedom of Information
- Directors and Non-Executive Directors
10.4 All staff should be aware that the system produces an electronic audit trail of access to and printing from the system.

10.5 Any electronic record / document which is printed from the system cannot, for any reason, be altered, deleted, added to or in any other way amended. All staff will be required to adhere to this practice and anyone found to have abused this may be investigated under the Trusts disciplinary policies.

11.0. ELECTRONIC RECORD DISPOSAL

11.1 Records may become eligible for disposal under retention schedules contained in the Records Management Code of Practice. This could be identified by calculating the dates of records within folders stored within a 'closed' or archive area of the folder hierarchy.

11.2 EDRM does provide more advanced Records Management functionality, where retention policies can be applied to folders. Staff can discuss use of this with the Systems Administrator.

11.3 Each department should conduct an annual records review. No records should be destroyed without Managerial approval ensuring that there is no need to retain specific records for any ongoing, planned or envisaged litigation, audit, investigation or open Freedom of Information request.

11.4 Special care must be taken with destruction of electronic records, which can be reconstructed from deleted information. Information can be leaked to outside persons through careless disposal of media, including exchange of media as part of a warranty and/or maintenance agreement. The method of media disposal should be based on the risks associated with the content held on the media.

11.5 Overwriting should ensure all previous information has been removed, but this should be done by authorised staff.

11.6 In some cases there will be more than one copy of a record. For example, there are likely to be back-up copies of records held electronically. A record cannot be considered to have been completely destroyed until all back-up copies have been destroyed, if there is any possibility that the data could be recovered.

11.7 For documents stored on the network, record the decision and destruction action and date in a spreadsheet document or database. Electronic systems will log all disposal actions within its audit trail.

11.8 The procedures within the CP9 Health Records Management Policy and CP9(g) Storage, Retention and Destruction of Records Procedure should always be followed, where appropriate for corporate records.

11.9 Records selected for archival preservation and no longer in regular use by the organisation should be transferred as soon as possible to an archival institution (The National Archives/Local Archive). Non-active records should be transferred no later than 20 years from creation of the record, as required by the Public Records Act 1958. Records, which are thought to be worthy of
permanent preservation, should be referred to the Trust Records Group for review.

12.0. REFERENCE TO OTHER POLICIES AND PROCEDURES

12.1 When processing records in any capacity reference should be made to any Trust policies relating to records as well as to local and professional guidance.

12.2 Other documentation will include:

- Health Records Management Policy and Procedures (CP9)
- Data Protection Act 2018 and Confidentiality Policy / Procedures
- Information Governance and Security Policy / Procedures
- Information Sharing and Consent Policy / Procedure
- Corporate Records User Guide for Laserfiche Document Management System *(NOTE – this will be supplied by the Scanning Team / Laserfiche once training is complete)*

*This list is not exhaustive....

END