INFORMATION LIFECYCLE MANAGEMENT POLICY, PROCEDURE AND STRATEGY

DOCUMENT CONTROL

<table>
<thead>
<tr>
<th>Version:</th>
<th>0.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ratified By:</td>
<td></td>
</tr>
<tr>
<td>Date Ratified:</td>
<td></td>
</tr>
<tr>
<td>Policy Author:</td>
<td>Essex CSU CCG IG Lead</td>
</tr>
<tr>
<td>Policy Sponsor:</td>
<td>Chief Finance Officer (SIRO)</td>
</tr>
<tr>
<td>Name of Responsible Committee:</td>
<td>Quality and Governance Committee</td>
</tr>
<tr>
<td>Date Issued:</td>
<td></td>
</tr>
<tr>
<td>Review Date:</td>
<td></td>
</tr>
<tr>
<td>Target Audience:</td>
<td>CCG Staff and Members</td>
</tr>
<tr>
<td>Equality Impact Assessment</td>
<td><strong>EQUALITY IMPACT ASSESSMENT</strong></td>
</tr>
<tr>
<td>---------------------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td></td>
<td>This document has been assessed for equality impact on the</td>
</tr>
<tr>
<td></td>
<td>protected groups, as set out in the Equality Act 2010. This Policy</td>
</tr>
<tr>
<td></td>
<td>is applicable to every member of staff within the CCG</td>
</tr>
<tr>
<td></td>
<td>irrespective of their age, disability, sex, gender reassignment,</td>
</tr>
<tr>
<td></td>
<td>pregnancy, maternity, race (which includes colour, nationality</td>
</tr>
<tr>
<td></td>
<td>and ethnic or national origins), sexual orientation, religion or</td>
</tr>
<tr>
<td></td>
<td>belief, marriage or civil partnership.</td>
</tr>
</tbody>
</table>
### Associated Policy/Procedural Documents

<table>
<thead>
<tr>
<th>Reference</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Data Protection and Confidentiality Policy</td>
</tr>
<tr>
<td></td>
<td>Information Governance Policy</td>
</tr>
<tr>
<td></td>
<td>Safe Haven Policy</td>
</tr>
<tr>
<td></td>
<td>Freedom of Information Policy</td>
</tr>
<tr>
<td></td>
<td>Information Security Policy</td>
</tr>
<tr>
<td></td>
<td>Information Risk Policy</td>
</tr>
<tr>
<td></td>
<td>Registration Authority Policy</td>
</tr>
<tr>
<td></td>
<td>Subject Access Request Policy</td>
</tr>
<tr>
<td></td>
<td>Pseudonymisation and Information Safe Haven Policy and Procedure</td>
</tr>
<tr>
<td></td>
<td>Business Continuity Strategy</td>
</tr>
<tr>
<td></td>
<td>Network Security Policy</td>
</tr>
<tr>
<td></td>
<td>Acceptable Use Policy</td>
</tr>
<tr>
<td></td>
<td>Forensic Readiness Policy</td>
</tr>
<tr>
<td></td>
<td>Mobile Working Procedure</td>
</tr>
</tbody>
</table>

### Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>BSI</td>
<td>British Standards Institute</td>
</tr>
<tr>
<td>CCG</td>
<td>Clinical Commissioning Group</td>
</tr>
<tr>
<td>CfH</td>
<td>Connecting for Health</td>
</tr>
<tr>
<td>CSU</td>
<td>Commissioning Support Unit</td>
</tr>
<tr>
<td>DOH</td>
<td>Department of Health</td>
</tr>
<tr>
<td>DQ</td>
<td>Data Quality</td>
</tr>
<tr>
<td>FOIA</td>
<td>Freedom of Information Act</td>
</tr>
<tr>
<td>FOIR</td>
<td>Freedom of Information Request</td>
</tr>
<tr>
<td>GP</td>
<td>General Practitioner</td>
</tr>
<tr>
<td>ILM</td>
<td>Information Lifecycle Management</td>
</tr>
<tr>
<td>IGSG</td>
<td>Information Governance Steering Group</td>
</tr>
<tr>
<td>KPI</td>
<td>Key Performance Indicators</td>
</tr>
<tr>
<td>KSF</td>
<td>Key Skills Framework</td>
</tr>
<tr>
<td>PDP</td>
<td>Personal Development Plans</td>
</tr>
<tr>
<td>SMS</td>
<td>Short Messaging Service</td>
</tr>
<tr>
<td>SARS</td>
<td>Subject Access Requests</td>
</tr>
</tbody>
</table>
Contents

1  Contents ................................................................................................................. 4
2  Objectives.................................................................................................................. 7
3  Scope ......................................................................................................................... 8
4  Accountability and Responsibility ........................................................................... 9
5  The Six Phases of the Information Lifecycle ............................................................... 10
5.1 Creation .................................................................................................................... 10
5.2 Naming ..................................................................................................................... 10
5.3 Filing Structure ....................................................................................................... 10
5.4 File Folder Referencing .......................................................................................... 11
5.5 Tracking and Tracing ............................................................................................... 11
5.6 Retention and Disposal .......................................................................................... 12
6  Creation and Management of Paper Records ............................................................ 13
6.1 Introduction .............................................................................................................. 13
6.2 Records Creation ..................................................................................................... 13
6.3 Records Maintenance ............................................................................................. 13
6.4 Records Archiving .................................................................................................. 14
6.5 Records Disposal ................................................................................................... 14
7  Creation and Management of Electronic Records ....................................................... 14
7.1 Introduction .............................................................................................................. 14
7.2 Document Naming .................................................................................................. 14
7.3 Folder Naming ........................................................................................................ 15
7.4 Version Control ...................................................................................................... 15
7.5 Version Numbering ............................................................................................... 16
7.6 Records Retrieval .................................................................................................... 16
7.7 Records Archiving .................................................................................................. 16
7.8 Records Deletion .................................................................................................... 16
8  Saving Electronic Documents ..................................................................................... 16
8.1 Introduction .............................................................................................................. 17
8.2 Saving to Local Hard Drive (C:) ............................................................................. 17
8.3 Saving to Network Personal Drive (P:) ................................................................... 17
8.4 Saving to Other Network Drives (usually S: or T: Drives) ........................................... 18
8.5 Structure of Shared Drives ................................................................................................................. 18
8.6 The Extranet ........................................................................................................................................ 18
8.7 Public-Facing Website ....................................................................................................................... 19
8.8 Removable Media .............................................................................................................................. 19

9 Document Scanning ............................................................................................................................... 20
  9.1 Introduction ........................................................................................................................................... 20
  9.2 Legislation and Standards .................................................................................................................. 20
  9.3 Responsibilities and Accountabilities ............................................................................................... 21
  9.4 Quality and Scale ............................................................................................................................... 21
  9.5 Standards for a Scanned Image ......................................................................................................... 22
  9.6 Standards for an Adobe Image ......................................................................................................... 22
  9.7 Document Retention ......................................................................................................................... 23
  9.8 Type of Document ............................................................................................................................... 23
  9.9 Disposal ............................................................................................................................................... 23
  9.10 Evidentiary Use of a Scanned Document ....................................................................................... 23

10 Data Quality ........................................................................................................................................ 24

11 Document Protective Marking ........................................................................................................... 24
  11.1 Introduction ........................................................................................................................................ 24
  11.2 Background and Classification Scheme Outline ............................................................................. 24
  11.3 NHS Confidential ............................................................................................................................. 26
  11.4 NHS Protect ..................................................................................................................................... 26
  11.5 Freedom of Information .................................................................................................................. 26

12 Management of Email .......................................................................................................................... 27
  12.1 Introduction ....................................................................................................................................... 27
  12.2 Emails as Records ............................................................................................................................ 27
  12.3 When is an Email a Record? ......................................................................................................... 27
  12.4 Storage and Filing of Emails ......................................................................................................... 28
  12.5 Printing Emails ............................................................................................................................... 28

13 Management of Outlook Calendar ....................................................................................................... 29

14 Maintenance of the Policy .................................................................................................................... 29

15 Monitoring and Compliance ................................................................................................................ 30

16 Information Lifecycle Strategy Objective ............................................................................................ 31

17 Strategy Implementation (Refer to Appendix A for list of actions) ................................................. 31
Appendix A - Future Actions ................................................................. 32
Appendix B: Rules of File-Naming......................................................... 35
Appendix C: Flowchart to Determine if Emails Have Value .................... 42
Appendix D: Classification of NHS Information – Marking Guidance ........ 43
Appendix E: Legal Acts Pertaining to this Document ............................. 44
Appendix F: Clinical Record Retention Periods .................................... 45
Appendix G: Corporate Record Retention Periods ............................... 46
Appendix H: Process Map for Scanning a Document Received Via Post ....... 48
2. Objectives

This policy will detail the processes that all employees should infuse, as a matter of routine, within their daily working practices in order to safely manage the organisation’s information throughout every phase of its existence, from creation through to disposal.

The Information Lifecycle Management principles apply to any information that may be held whether held on paper or on any other formats, inclusive of but not limited to; electronic, microfilm, audio and video. The lifecycle of information covers 6 different phases; creation, naming, filing structure, filing/organisation, tracking and tracing and retention/disposal.

This Information Lifecycle Management policy, procedure and strategy will incorporate all aspects of Records Management and will provide the broad guidance for Information Management, as detailed within the scope of this document.

The objectives of this policy, procedure and strategy are to:

- Provide an explanation of the six phases of the Information Lifecycle (as detailed within the Information Governance Toolkit) from creation through to disposal.
- Provide guidance on how and where electronic records should be saved on the network/s.
- Provide guidelines as to record naming and version control.
- Provide examples as to best practice for record naming.
- Provide further points of reference for staff and legal directives.
- Provide the detail for future actions to be addressed by each of the CCG’s.

The CCG must have policy and management processes implemented, that are in line with the both the requirements of the organisation, and the Information Governance Toolkit in order to effectively manage the information that is created and held within.

Information is a vital business asset. Healthcare professionals are highly reliant on quality, up to date accurate information in order to protect the clinical safety of their patients, and to provide healthcare of the highest quality. Commissioners must be provided with relevant, timely, accurate information in order to manage effectively consultation processes and to make well informed decisions concerning priority setting and service provision. Therefore information should be kept accurate, up to date and secure, and when requested easily retrievable and available to those who need access.
Whilst this policy contributes towards meeting the fundamental requirements of the DoH Information Governance Toolkit, it is also a guide for all employees to follow when dealing with associated issues of the security of person identifiable information, the use of information in accordance with the Data Protection Act 1998 and the Freedom of Information Act 2000.

The guidelines detailed within this Policy, Procedure and Strategy will help to ensure that the organisation protects its information assets from being compromised. Anyone found deliberately or negligently violating this policy may be subject to disciplinary action that could ultimately lead to their dismissal.

3. Scope

This over-arching policy covers all information types, clinical, non-clinical, person identifiable, records of all types including corporate information* regardless of the media on which they may be held. These records may consist of:

- Patient health records (electronic or paper based, including GP records)
- Records of private patients who may be seen/receive treatment on NHS premises
- Minor Injury units and the Walk-in-Centre, birth and all other registers
- Theatre registers and minor operations (and other related) registers
- *Corporate records
- X-ray and imaging reports, output and images
- Photographs, slides and other images
- Microform (i.e. microfiche/microfilm)
- Audio and video tapes, cassettes, CD-ROM etc.
- E-mails
- Message books and diaries
- Computerised and scanned records
- Text messages (inclusive of both outgoing SMS's from an NHS organisation and incoming responses from the patient)

*Corporate information is information that may be created during the course of duties by the CCG, that is not of a clinical nature, or in anyway patient identifiable information. Corporate records/information is information created that relates to the organisation’s business activities and therefore will include records from the following functions of the CCG.

- Finance and procurement
- IM&T
• Information Governance
• Human Resources, OD and training
• Performance management
• Corporate Governance
• Health care quality and clinical audit
• Commissioning and contracts
• Complaints and compliments
• Communications and Patient Advisory Liaison Service
• CCG Board business

Examples of corporate information:

• Policies and procedures
• Strategies and action plans
• Minutes and agendas
• Reports (e.g. annual, accounting, Board)
• Financial Standing Orders
• Public consultations
• Databases
• Contracts

For records audit purposes, the definition of what constitutes a CCG Corporate Record may include a grouping of CCG documents i.e. a folder full of individual project related documents could be considered a single Corporate Record of that project.

The Policy will make reference to, and be supported by, other policies and guidelines which will provide the relevant detail needed in specific areas. A list of these supporting policies and guidelines can be found detailed at the beginning of this document on Page three.

4. Accountability and Responsibilities

It is the responsibility of all CCG employees to adhere to this policy when handling all types of CCG information. Training will be provided as part of the staff induction process and forms part of the staff annual PDP discussions with line managers.

Employees should familiarise themselves with this policy and any other related policies, in order to ensure they are aware of their own individual responsibilities. Adherence to this policy
and related policies also forms part of the employees’ employment contract and annual appraisal process.

All NHS employees are responsible for any records that they may create or use within the course of their duties. Records created by an employee of an NHS organisation, are in effect public records and are therefore subject to both legal and professional obligations.

The Essex Information Governance Steering Group (IGSG) is responsible for the development, maintenance and regular review of this policy and reports to the Senior Information Governance Officer (SIRO) which reports to the CCG Board. The CCG’s SIRO will take the lead on Records Management. This role will also lead on performance management, records management audit to ensure required standards are maintained at all times.

5. The Six Phases of the Information Lifecycle

The Information Lifecycle has six phases:

1. Creation
2. Naming
3. Filing Structure
4. File Folder Referencing / Organisational
5. Tracking and Tracing
6. Retention and Disposal

5.1 Creation

- Record creation is one of the most important processes in records management and all staff within the organisations should aim to create good records that can be used in an effective system. However, creating a record is not sufficient enough unless the record is then captured or filed into a filing system that is both effectively created and managed.
- It is important that records are kept in their context and the best way to achieve this is to ‘file’ or ‘classify’ them. Records cannot be tracked or used efficiently if they are not classified or if they have been classified inappropriately. Records captured or filed in a corporate filing system must contain some of the necessary characteristics to be regarded as authentic and reliable. Whatever the format of the records, they must be saved into an organised and structured records management system.
- A common format for the creation of records will ensure that those responsible for record retrieval are able to locate records more easily.
- When staff create corporate records, a common format should always be used that as a minimum includes:
  i. the difference between a document and a record;
  ii. the referencing to be applied to any new records;
iii. the version control standards to be followed;
iv. the agreed naming conventions within use in the CCG;
v. where an original record should be filed;
vi. how to apply a protective mark to a record, (if appropriate).

5.2 Naming

All Staff should ensure that naming conventions must:

- 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 manner and predictable order;
- locate the most specific information at the beginning of the name and the most general at the end;
- provide a similarly structured and worded name to all records which are linked (for example, an earlier and a later version).

5.3 Filing structure

- A clear and logical filing structure that aids the retrieval of records must be used. The filing structure should reflect the way in which paper corporate records are filed to ensure consistency. However, if it is not possible, the names allocated to files and folders should allow ‘intuitive filing’. Filing of the primary corporate record to local drives on PCs and laptops is not permitted.
- The agreed filing structure will also help with the management of the retention and disposal of records.

5.4 File/Folder Referencing

- A referencing system that fulfils the organisation’s business needs must be used. It must also be taken in consideration, to ensure that the system is to be user friendly so that it can be easily understood by all staff members that may create documents and records. Several types of referencing may be used, for example, alphanumeric; alphabetical; numeric; keyword, etc. The most common of these is alphanumeric, as it allows letters to be allocated for a business activity, for example, HR for Human Resources, followed by a unique number for each record or document created by the HR function.
- In some circumstances, it may be more feasible 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.
- Regardless of which method is used, it should be agreed and understood by all concerned and be in line with business needs of the department.
5.5 Tracking and Tracing

- Tracking and tracing procedures implemented must enable the movement and location of records to be controlled. This will provide an auditable trail of record transactions. The process need not be a complicated one, for example, a tracking procedure could comprise of a book that staff members sign when a corporate record is physically removed from or returned to its usual place of storage (not when a record is simply removed from a filing cabinet by a member of staff from that department as part of their everyday duties).

Tracking mechanisms to be used should include:

- the item reference number or identifier;
- a description of the item (for example the file title);
- the person, position or operational area/team who may have possession of the item;
- the date and time of movement that took place

Systems that may be used in order to monitor the physical movement of records, are as follows:

- location cards;
- index cards;
- docket books;
- diary cards;
- transfer or transit slips;
- bar-coding;
- computer databases (electronic document management systems);
- regular record audits.

The system adopted should maintain control of the issue of records, the transfer of records between persons or operational areas, and return of records to their home location for storage. The simple marking of file jackets to indicate to whom the file is being sent is not in itself a sufficient safeguard against files going astray.

5.6 Retention and disposal

Retention/disposal procedure must be based on the retention schedules as detailed within the Records Management: NHS Code of Practice. Schedules are to be arranged based on series or collections of records and must indicate the appropriate disposal action for all records (for
example consult with a local place of deposit or The National Archives after ‘x’ number of years).

Records selected for archival preservation that are no longer in regular use by the CCG are to be transferred as soon as possible to an archival institution (for example a ‘Place of Deposit’, that has adequate storage and public access facilities. Non-active records should be transferred no later than 30 years from creation of the record, as required by the Public Records Act 1958.

Methods to be used throughout the destruction process will provide adequate safeguards against the accidental loss or disclosure of any contents of any records that are to be destroyed. When contractors are used, they will be required to sign confidentiality undertakings and will produce authenticated certificates as proof of destruction, for each destruction episode that takes place.

A record of the destruction of records, showing their reference, description and date of destruction will be maintained and preserved, so that the CCG can accurately identify which of those records that have been destroyed and are therefore no longer available. Disposal schedules will constitute the basis of such a record.

6 The Creation and Management of Paper Records

6.1 Introduction

This section will detail how paper records are to be created and will include specific guidance on referencing, naming, filing and protective marking.
It is important to clearly detail the difference between a record and a document. A document, effectively becomes a record once it has been finalised and becomes part of the CCG’s corporate information.

6.2 Records Creation

All paper records must be identified clearly on the front cover with an accurate title and description and where appropriate, the department or service and the name of the author of the record.

6.3 Records Maintenance

All corresponding information contained within the record/s should be arranged in a logical structure and be ordered chronologically. Duplicate papers should be removed and where a file becomes too large, or difficult to manage, a second volume should be created.

All services and departments, within the CCG should devise a file-plan to keep track of the records they hold within. The approach to this must be consistent. This will also assist with records auditing. The file-plan should be reflected in the physical storage of the files.
Information held within corporate paper records may be required as part of a response to a request under the Freedom of Information Act 2000. By law, such requests must be processed within specific time limits (20 working days). Therefore records should be easily accessible and available to authorised members of staff.

Records must be stored securely, and under no circumstances left unattended or accessible to staff who do not have the authority to see them. When records are removed from the office, a tracking system should always be kept, detailing who has removed the record and where it has been taken to (name/team/department/time/date).

6.4 Records Archiving

Records that are no longer in day to day 'use' (inactive) should be earmarked for archiving and sent to the CCGs archive facility at To be added

Staff should follow the guidelines set out in the To be added

6.5 Records Disposal

Disposal of obsolete records should be undertaken once they have exceeded the retention periods as stipulated within the 'DoH Records Management Code of Practice Part 2', an extract of which is available at appendix F and G in this policy. In a few, select cases, records which are deemed to be of historical value, may be sent to the National Archives for purposes of preservation.

7 The Creation and Management of Electronic Records

7.1 Introduction

This section will detail the procedures for ensuring that electronic corporate records are accessible and retrievable as and when required. It will not only cover electronic documents on stored on network drives and shared folders, but also emails, attachments and documents embedded within web pages. The section will also provide instruction on how to save documents, use naming convention and version control.

7.2 Document Naming

‘File names’ are the names that are listed within a computer’s file directory, that users may give to new documents when they save them for the first time, following creation. Naming documents in a consistent, logical and predictable way will distinguish similar records from one another at a glance, and should contribute towards correct location and easy retrieval. Naming documents according to an agreed convention should also make file naming easier for colleagues because they will not have to rethink the process each time. The key is to keep it as simple and user friendly as is feasibly possible.
There are 11 rules to follow (see Appendix B for further guidance):

1. Keep file names short, but meaningful;

2. Avoid unnecessary repetition and redundancy in file names and file paths;

3. Use capital letters to delimit words, not spaces or underscores;

4. 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;

5. 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;

6. When including a personal name in a file name give the family name first followed by the initials;

7. 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;

8. Order the elements in a file name in the most appropriate way to retrieve the record;

9. 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 these elements would be incompatible with rule 2;

10. 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 rule 2;

11. The version number of a record should be indicated in its file name by the inclusion of ‘V’ followed by the version number and, where applicable, the terminology ‘Draft’ should be used.

7.3 Folder Naming

As with the naming of documents, folders should be named in a logical way. Avoid personal names, vague or general titles such as ‘Various’, ‘Miscellaneous’, ‘Dave’s Files’ etc. Folder names should relate to topic or subject area, service or department /team name. Care must be taken so that a single folder should not be filled with hundreds of documents. If possible, a sub-folder structure should be utilised to help facilitate a rapid location of a desired document.
7.4 Version Control

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, simultaneously and those changes may not always be immediately apparent.

Version control is also very important when working on a collaborative document with a number of contributors and/or frequent revisions, for example a document that may be subject to an ‘on-going’ consultation response.

7.5 Version Numbering

Always use a unique version number to distinguish one version from another. This procedure is to be used for all documents where more than one version exists, or is likely to exist at some point in the future. This system should use version numbers with points to reflect major and minor changes with examples as follows:

Version 0.1 – Initial Draft
Version 0.2 – Revised Draft
Version 1.0 – Final Document
Version 1.1 – Subsequent minor change to Final
Version 2.0 – Major revision to Version 1.0

The version number should be recorded on the document cover and on the footer of each page.

7.6 Records Retrieval

When opening an electronic record, care must always be taken, to ensure that the correct version is being opened where multiple versions may exist. Thought should be given to archiving off old versions of a record to a different folder to simplify the folder contents for future usage.

7.7 Records Archiving

Thought should be given to the preservation of historic electronic records. Folders that are no longer in day to day use should be moved to an archive area of the shared drive and renamed to reflect the fact that they are now archived and not in daily use.
7.8 Records Deletion

Electronic records are subject to the same terms as paper records with regards to their retention periods. Reference should be made to the retention periods as stipulated in the *NHS Records Management Code of Practice - Part 2* an extract of which is attached in appendix F and G of this policy.

8 Saving Electronic Documents

8.1 Introduction

When saving a document, care must be taken to ensure that documents are saved to the correct location, from which they can easily be retrieved as and when required.

8.2 Saving to Local Hard Drive (C:)

Documents should not be saved to the local C: Drive. This local drive is not backed up and any documents stored on it will be lost in the event of hardware failure or computer theft. Staff should be aware that on many computers this is the default (i.e. automatic) setting which is an inappropriate location for saving corporate (or any) documents to.

The only exception to this rule is when staff do not have access to a network drive and have no option but to save to the C: Drive. Staff must ensure that, in this event, the computer is encrypted with either Safeboot or an alternative encryption software method and the document is saved onto the network as soon as possible.

8.3 Saving to Network Personal Drive (P:)

The Personal Drive (P: Drive) is the space on the network which is allocated to each member of staff and is accessible only to them. Information saved within this drive should be information that only the individual member of staff may need access to e.g. Staff appraisal information, privately stored personal materials such as a C.V etc.

Information created on the P: Drive is secure and is backed up every day. The individuals P: Drive is mapped to their logon and is accessible only to the individual from any location or computer linked to the network that they may logon to.

When the staff member leaves the organisation, the information on their P: Drive must be either transferred to a department shared folder or to the P: Drive of a colleague or line manager. Any information no longer required should be deleted.

Records created which provide evidence of the CCG’s activity should be saved on the shared drive as a CCG held record.
Information stored on the individuals P: Drive should be reviewed regularly to see whether it needs to be deleted or transferred to a folder on the shared drive in line with the Records Retention Schedule.

**Examples of Documents which should be held on the P: Drive**
- Individual’s KSF Outline
- Individual’s training, development and appraisal records
- Documents which need to be referenced only by the individual.

**Examples of documents which should not be held on the P: Drive**
- Finalised (V1.0 OR V2.0) CCG documents
- Any document which is considered to be a CCG record.
- Draft documents which others may require access to in the course of their duties.

**8.4 Saving to Other Network Drives (e.g. S:, T:, X: Drives)**

Departments/Teams should maintain a shared network drive which is accessible only to members of that department or team and any other individuals whom the department may decide to grant access to.

A shared network drive will enable all members of a department or team to access documents contained on the drive and is the best way for departments to hold their information as it will enable quick access to requests for information and makes records management easier as similar records can be grouped together in a folder structure. The shared network drive is secure and is backed up every day. Shared network drives are usually mapped as S: T: or X: Drives, but may have other letters depending on where, and how it was mapped. Requests for shared drives should be made to the IM&T helpdesk.

Consideration should be carefully given to user permissions as not all users may require the same level of permission/access - i.e. some users may only require read-only access where as others may require edit/read/write/delete.

**8.5 Structure of Shared Drives**

Folders at the top level of the shared drive (the ‘root’) should be created by the IM&T Helpdesk. These folders will be created with the necessary permissions to protect the confidentiality of the information contained within. Only nominated individuals should have access to the folders and these permissions should be set accordingly at the correct level i.e. individuals that only need to read documents in a particular folder should be set up to have ‘read-only’ permission, whereas individuals that may need to update or add new documents to a folder should have ‘read/write’ permissions. ‘Read/write/delete’ permissions should only be given to the individuals who need them.

Sub folders should be set up in a logical way to reflect the work activities of the department.
8.6 The Extranet

The Extranet is a web-based communication tool. It has been set up in a centralised location, to enable staff to easily locate any materials that they may need. This is to help them carry out their duties or to generally find out more information on a particular subject.

Examples of information which should be published on the Extranet are:
- Policies, Procedures and Strategies
- Forms
- Contact Lists
- Minutes of Meetings
- General Information
- Newsletters

Examples of information which should not be published on the Extranet are:
- Confidential Information
- Patient / Personal Information
- Commercially Sensitive Information
- Incomplete Information e.g. draft documents

8.7 Public-Facing Website

Information that is intended to be made publicly available should be published through the FOI publication scheme located on the Public-Facing Website. Requests for new content to be added should be made via the CSU FOI Co-ordinator.

Examples of information which should be routinely published on the public-facing website are:
- CCG Annual Report
- Press Releases
- Up to date contact Information for the CCG
- Information about services provided by the CCG
- A list of the main categories of Information that have been most frequently requested via the FOIA
- A list of Data Sets requested previously under the FOIA

Examples of information which should not be published on the public-facing website are:
- Person Identifiable Information of any description
- Confidential Reports
- Commercially Sensitive Information
- Incomplete Information e.g. draft documents, any information not approved or finalised
8.8 Removable Media

There may be circumstances where CCG documents will need to be stored on removable media. The use of this media needs to be strictly controlled in order to maintain confidentiality. For instructions on the correct use of removable media, please see the Information Security Policy.

9 Document Scanning

9.1 Introduction

Legal requirements and good practice demand that paper records are retained for future reference or evidence until the time comes when they can be destroyed. This is determined depending on classification of the information contained within. This has the potential to generate considerable physical storage requirements in environments which have only limited storage space available. One way to overcome the physical storage space issue is to scan the paper document into an electronic system and save it to an agreed location (known as becoming 'paperlight'). To ensure the scanned documents remain admissible in a court of law certain standards have to be met. This does not guarantee the document is admissible in a court of law but standard BS 10008 (Evidential Weight and Legal Admissibility of Electronic Information) has been referred to, for example, in the Lord Chancellor's Code of Practice on the Management of Records where he states that ‘authorities should seek to conform to this standard, particularly for those records likely to be required as evidence’.

9.2 Legislation and Standards

Standards exist concerning the use of scanned documents:

Civil Evidence Act 1995, Section 8 and 9

8 (1) Where a statement contained in a document is admissible as evidence in civil proceedings, it may be proved;

(a) by the production of the document, or

(b) whether or not that document is still in existence, by production of a copy of that document or of the material part of it, authenticated in such a manner as the court may approve.

(2) It is immaterial for this purpose how many removes there are between a copy and an original.
(1) A document that is shown to form a part of the records of business or a public authority may be received in evidence in civil proceedings without any further proof.

(2) A document should be taken to form part of the records of a business or public authority if there is produced to a court a certificate to that effect signed either by an officer of the business or authority to which the records belong.

Legal Admissibility and Evidential Weight of Information Stored Electronically, British Standard – BSI DISC PD008

BSI BIP 0008 is a code of practice that provides guidance to ensure, as far as possible, that electronic documents and scanned images will be accepted as evidence by the courts. The key to this guidance is that the process under which documents are managed is as important as the technology used – where a document is reproduced it should accurately reproduce the contents of the "original".

The key points are listed below;
- Recognise and understand all types of information – implement an information management policy
- Understand the legal issues and execute ‘duty of care’ responsibilities
- Identify and specify business processes and procedures
- Identify enabling technologies to support businesses and procedures
- Monitor and audit business processes and procedures

British Standard BS 10008

BS 10008 has been referred to in the Lord Chancellor's Code of Practice on the Management of Records where he states that ‘authorities should seek to conform to this standard, particularly for those records likely to be required as evidence’.

Also, the Cabinet Office website states that ‘this British Standard lays down the process required when converting paper records to legally admissible electronic records’.

9.3 Responsibilities and Accountabilities

Heads of Service have overall responsibility to ensure this policy and associated standards are complied with at all times, by all staff.

Team Leaders and Managers are responsible for ensuring that all staff do attend relevant/mandatory annual training on information governance. Also to ensure that staff understand this policy and follow procedures associated with storing electronic documentation.

Staff employed by the CCG are responsible for adhering to policies and procedures concerning scanning. It is also the individual staff member’s responsibility, to report any problems or training issues that occur to their line manager immediately.
9.4 Quality and Scale

The Codes of Practice on the Management of Records, notes that large drawings and maps may be processed after scanning to correct scale inaccuracies; if this is done then the uncorrected paper version should also be kept. It also notes that where the original document is of poor quality or contains physical amendments that cannot be identified as an amendment on a scanned image, the original should be kept along with the duplicated copy.

Some documents may not be able to be scanned in accordance with the high standards set out within the British Standard. For example, if the technology is not available to the CCG to produce a true copy of x-rays, colour documents, old handwritten documents in faint type, oversized documents etc., these should be retained in paper format. The standard and its Codes of Practice note particular issues with scanning some documents, such as x-rays, and the technical specifications that must be met to achieve compliance.

9.5 Standards for a Scanned Image

Images must adhere to the following standards;

- Every image must be a true representation of the original document
- All text must be legible.
- The patient/staff member associated with the document must be clear on the scanned image.
- All images received from an external source must be date stamped, when received, before scanning into electronic form. This must be clear on the scanned document.
- There must be an audit trail on the system of the date and time when the image was scanned into the system.
- There must be a completed audit trail of information detailing who scanned and saved the image into the system, inclusive of time/date.
- The image should be saved to a suitable agreed resolution to ensure quality.
- An audit trail must be kept, detailing destruction of any documents. The best practice process would be to retain the original information with the scanned image.

For a process map to scan a document received via post, please see Appendix H

9.6 Standards for an Adobe Image

Documents may be converted into an ‘Adobe’ image and saved like a scanned image. However, images must adhere to the following standards:

- Every image must be a true representation of the original document
- All text must be legible
- The patient / staff member associated with the document must be clear on the image
- There must be an audit trail on the system of the date and time when the image was saved into the system.
- There must be an audit trail of who saved the image into the system.
- The image should be checked before it is saved to ensure quality.

9.7 Document Retention

To ensure systems have saved the images and have been backed up, documents should be kept for seven days afterwards, before the confidential disposal takes place. While these documents are awaiting disposal they must be kept in a secure location as they contain confidential information.

9.8 Type of Document

This is not intended to be a definitive list but can be used for reference.

<table>
<thead>
<tr>
<th>Type</th>
<th>Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee Records</td>
<td>Scanned into a document management system to be saved under the correct criteria</td>
</tr>
<tr>
<td>Financial documents</td>
<td>Scanned into a document management system to be saved under the correct criteria</td>
</tr>
<tr>
<td>Correspondence</td>
<td>Scanned into a document management system to be saved under the correct criteria</td>
</tr>
<tr>
<td>Complaints Letters</td>
<td>Scanned into a document management system to be saved under the correct criteria</td>
</tr>
</tbody>
</table>

9.9 Disposal (Scanned Documents)

All scanned documents containing patient, staff or financial information must be disposed of in a confidential manner, using a confidential waste disposal service/ or by means of a cross cut shredder to the specification of DIN level 3. The documents should only be destroyed after the guidance in this document has been followed and a full review has taken place.

A detailed audit trail should be kept of when the document was destroyed. This should also be recorded on either the clinical system or document management system to aid the audit trail.

Where fraud is suspected, original documents should not be destroyed until after any criminal investigation/ litigation has been completed, as destruction of documents in this context could constitute a criminal offence. All staff should be mindful of this. Also, some authorities (such as
the HM Revenue and Customs) expect records that they audit to be retained in paper format regardless of whether they have been scanned onto a system.

9.10 Evidentiary Use of a Scanned Document

If a document is needed, as evidence to be used in court, by checking the record a senior manager can then certify what policy/procedure was in place for the scanning of that documents, and that they have checked that this document was recorded as destroyed and the scanned image is recorded as a true copy of the original document.

An audit trail must exist of all destroyed documentation and the processes and procedures that have been implemented. If required by the court, evidence may be requested that may need to be presented to the court to assist with a particular case. Staff should be mindful of this scenario arising, and this should be considered prior to any destruction of any materials taking place.

10 Data Quality

Data quality is of crucial significance to the CCG, the availability of complete, accurate and timely data is of utmost importance in supporting the delivery of patient care, clinical governance and service agreements for healthcare planning. The availability of good quality data is absolute key to the monitoring and measurement of the CCG’s performance targets.

The increasing use of computerised systems provides greater opportunities to store and access data but also consequently increases the risk of misinformation if the data is not of a high standard. This risk applies not only to the internal use of information but to information used for the completion of statutory returns to the national databases. For this information to have value it is essential that the underlying data is consistent and compliant with data quality standards.

11 Document Protective Marking

11.1 Introduction

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. For example, at some 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 may also hinder the development of appropriate IT system protocols.
11.2 Background and Classification Scheme Outline

This section sets out a simple scheme of classification relevant to the needs of NHS organisations. 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 activities and the kind of information used between the NHS and other public sector environments. The NHS does not have a requirement for the full range of protective markings as used within U.K. Government. For example, central Government uses six categories of information classification: Top Secret, Secret, Confidential, Restricted, Protect and Unclassified and these are more relevant within an NHS context. 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.

11.3 NHS Confidential

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 – Part 1 and 2). Therefore, the marking NHS CONFIDENTIAL should be used for that kind of information (e.g. patients’ clinical records, patient identifiable information, and information about NHS staff that is communicated between NHS staff, and between NHS staff and staff of other appropriate, authorised and approved agencies). This may include patient demographic details that might identify people who have had a GP episode/contact/hospital appointment within a particular timeframe or who may have a particular condition. PLEASE NOTE: In order to safeguard confidentiality, the term “NHS Confidential” should never be used on the correspondence (packaging i.e. envelope) to a patient. ‘Private and Confidential’ should be used.

The endorsement NHS CONFIDENTIAL should be included at the top centre of every page inside the document. Documents marked so, should be held securely at all times. They should be stored in a locked room or equivalent (lockable cabinets, held within secured electronic systems to which only authorised persons may be provided with access. They should not be left unattended at any time in any locations where unauthorised persons might be able to gain access to them. They should be transported securely in sealed (lockable) containers or wallets and not left unattended at any stage. There are no allowances or exceptions. Documents that are marked as ‘NHS CONFIDENTIAL’ not kept in a designated safe store or transport facility should always be kept out of sight of visitors or others who are not authorised to view them. For further guidance please refer to the Safe Haven policy.

Other uses of NHS Confidential:

The endorsement NHS CONFIDENTIAL should also be used to mark any other information of a sensitive nature: material that the disclosure is likely to:
● adversely affect the reputation of the organisation or its' officers or cause substantial distress or harm 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;
● dis-advantage the organisation in commercial or policy negotiations with others or undermine the proper management of the organisation and its operations.

A paper, printout or report etc. marked as 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 ‘Appendix D’ at the end of this document. The endorsement should be included at the top centre on every page of the document. All NHS CONFIDENTIAL documents should be stored in lockable cabinets or secured electronic systems with appropriate safeguards..

Information may be classified as ‘NHS CONFIDENTIAL’ in light of the circumstances at any one given particular time. The classification should be kept under review and the information de-classified as and when the need for this protection is no longer deemed necessary. NHS use of an equivalent classification for “Restricted” is unnecessary when NHS CONFIDENTIAL is used.

11.4 NHS Protect

In Government the classification of marking “PROTECT” is discrentional marking, which may be used in order to avoid unauthorised access to certain types of information. It establishes the basic principles to be followed to ensure that information is handled with care, taking the relevant precautions and to ensure that it is disposed of in a safe manner.

In the NHS context, it is therefore possible for NHS organisations to adopt and use an equivalent level of classification “ NHS PROTECT” marking, with or without descriptors, for information that requires protection below that of standard NHS CONFIDENTIAL , but where care in handling is still deemed to be necessary. Departments and Service Areas that choose to adopt NHS PROTECT must therefore ensure their staff and business partners are aware of the difference in expectations and arrangements that apply for the protection and assurance of NHS CONFIDENTIAL and NHS PROTECT, labeled information.

11.5 Freedom of Information

When classifying NHS documents, consideration must always be given to the requirements of the Freedom of Information Act 2000. Extra careful consideration should be given before
marking documents that would normally be published or disclosed on request. Over-classification may well lead to an inappropriate decision not to disclose information that would later be embarrassing to the organisation (for example, in a scenario where there was an appeal against the non-disclosure decision or the Information Commissioner became involved and subsequently the initial decision was overturned). Protective markings should, wherever possible be restricted to information that would be exempt from disclosure, including temporary exemption, such as that for drafts of documents that are intended for publication.

A note of the exemptions that might be relevant to the protective markings is included within ‘Appendix D’ at the end of this document. However, nothing in this guidance should be taken as an authoritative guide on the operation of the Freedom of Information Act 2000. Further information about the Act and its exemptions (including the application of the “public interest” test) is available on the website of the Information Commissioner (www.informationcommissioner.gov.uk), and also from the CSU Information Governance Team.

12 Management of Email

12.1 Introduction

It is important to remember that while email is a vital important tool for communication, it is not designed to meet Records Management standards or long term storage requirements. Email is, however, probably the primary means by which the CCG conducts its business arrangements and may be used for such things as communicating important documents, confirming actions, giving permission for certain actions, conveying information to those authorised and in need and general messages. Emails are in fact business records which may be open to scrutiny under the FOIA and may be required for evidential purposes. Staff should be mindful of this, at all times, therefore emails should be filed in a categorised, organised structure that will facilitate easy retrieval upon receiving a request for information.

12.2 Emails as Records

Emails have a value as organisational records and they therefore have a requirement to be managed in accordance with the DoH Records Management Code of Practice and are to be retained for the period of time determined within the Code.

12.3 When is an Email a Record?

It is important to distinguish between different categories of emails and determine which emails are to be retained (as they may be requested via FOIA) or as evidence for other purposes, and which can be safely deleted. Appendix C at the end of this document contains a flowchart to assist you.
Failure to understand this process may result in important records being prematurely deleted or retained for longer than is actually necessary, and this would contravene the retention and disposal schedules as stated within the DoH Records Management Code of Practice Part 2.

**Core Business Records**
These emails contain information on core business activities. They may need to be retained for both, operational or legal reasons and they may need to be referenced by others. Examples of this type of email may include:

- Expression of approval of a particular action or decision
- Direction for important actions or decisions
- External business correspondence
- Justification/s of decision making
- Policy precedents

The retention period for emails in this category should be in line with the retention periods, as stated in the DoH Records Management Code of Practice Part 2.

**Emails Containing Personal Data**
These emails contain information about specific individuals such as patients and staff and should always be sent via NHS.netmail. ‘NHS.net’ is the only recommended and approved method for sending person identifiable information by email in the NHS to another NHS member of Staff. Please note that the recipient email domain would also have to be NHS.net.

**Reference Records**
These are work-related emails with a transitory value which may need to be retained, but only in the short term. Examples of this type of email may include:

- Records for information such as staff on duty/holiday etc.
- Invitations and responses to work-related events
- Meeting notices and arrangements
- Copies of reports, minutes etc.
- Copies of newsletters
- Cover letters (“please find attached…”)
- Internal email messages received as c.c. or b.c.c.

### 12.4 Storage and Filing of Emails

Emails which are records, or which need to be shared with colleagues, should be filed alongside other documents in their business context and any relevant attachments. For example, if the main file is paper-based, then relevant emails should be printed and added to it and the original email deleted. If the main files is on a network drive, emails and attachments should be saved as text files to that area.
**Outlook Email Accounts**
Users are limited to a certain amount of storage in their Outlook email mailbox. For this reason, regular housekeeping of emails is required. Emails may be retained within structured Personal Folders (.pst) within Outlook. For assistance in creating a Personal Folder please contact the IM&T Helpdesk.

**NHSmail Accounts**
Users are limited to the amount of storage in their NHSmail mailbox. Users have the ability to create additional folders within their mailbox for sorting of emails but this will still contribute to the overall size. If you are using NHSmail as your main email account and are viewing these emails via Outlook, you can also create Personal Folders as above. It is recommended that users regularly carry out housekeeping of their NHSmail Mailbox to ensure that size limits are not exceeded and accounts are not suspended.

### 12.5 Printing Emails

Printing should be avoided unless:
- There is an effective paper file storage system in place
- Working files require all information to be kept together

If printing, ensure that the name of the email sender, all recipients and date/time of transmission or receipt are printed without alteration.

Additionally, the following rules should be observed:
- Avoid printing documents sent for information (c.c.) only
- File the printed version in the appropriate file
- Ensure copies are destroyed according to the retention schedules
- Avoid duplication – if email is printed, delete the electronic version

### 13 Management of Outlook Calendar

Users of email will book appointments and meetings via the Microsoft Outlook Calendar. The historic information contained within this calendar will accumulate over period’s time and will contribute to the size of the user’s mailbox – especially if attachments are contained in meeting invites. It is recommended that information is either archived or deleted (user’s discretion) after two years using the following method:

Right Click on the ‘Calendar’ entry in ‘My Calendar’

Select ‘Properties’ from the list of options
Select the ‘AutoArchive’ tab
Click on the ‘Archive the folder using these settings’ option
Set the ‘Clean out items older than…’ entry to 25 months or as is desired
Select either ‘Move old items to…’ or ‘Permanently delete’ at user’s discretion
If items are moved, it is recommended that they are moved to the same location as any existing email archive (*.pst) folder
14 Maintenance of the Policy

This Information Lifecycle Policy & Procedure will be reviewed bi-annually and will be approved by the Information Governance Steering Group. It may also be reviewed as and when new technologies, systems, ways of working or government or legal directives demand it. Prior notification of a review taking place may not be provided.

15 Monitoring and Compliance

It is the responsibility of all CCG staff to ensure compliance with this policy and procedure. This will be monitored by utilising the following methods:

- Annual Records Management audits
- Monthly checks on server folder structures and permissions

Device Control software will also be deployed at a future date which may restrict the use of USB storage devices and also restrict the type of data which may be emailed, copied and printed.

Basic Records Management training will be undertaken as part of IG Training.

16 Information Lifecycle Strategy Objectives

The objectives of the strategy are to ensure:

- That the CCG fulfils its obligations in becoming a paper light organisation, continuing to build upon the strong foundations implemented by PCT’s
- To implement a systematic, consistent and planned approach to the control and use of information throughout its whole lifecycle, from creation through to disposal across all CCGs
- An increase in efficiency, through improving the quality of the information held, the flow of that information to those authorised and greater co-ordination of management and storage of information
- Compliance with statutory requirements: The Freedom of Information Act, The Data Protection Act and Access to Health Records Act
- Adherence to NHS best practice standards
- Staff awareness of the importance of the information being collected and held by the CCG and their obligational duties when handling information

17 Strategy Implementation

The action points, in the table detailed in Appendix A (below) have been developed to form the basis of the implementation of this strategy and intend to create a clear starting point from which to build upon. Information lifecycle management covers an extremely broad scope and is CCG wide, across all aspects of information. It will be an evolving strategy to be continually developed, as constraints and requirements change throughout the future.
## Appendix A – Future Actions

<table>
<thead>
<tr>
<th>Objective</th>
<th>Action</th>
<th>Date Action Created</th>
<th>Owner</th>
<th>IG Toolkit Ref</th>
<th>Date of Completion</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>A</strong>-Accountability</td>
<td>Implement and maintain Asset Register to provide clear system of accountability for all information held by CCG</td>
<td></td>
<td></td>
<td>(345)</td>
<td></td>
</tr>
<tr>
<td><strong>B</strong>- Support and Management Approval</td>
<td>Ensure Senior Management ownership and commitment to the implementation of the ILM strategy</td>
<td></td>
<td></td>
<td>(345)</td>
<td></td>
</tr>
<tr>
<td><strong>C</strong>-Training</td>
<td>1) Ensure Information Lifecycle practices are included in Staff Induction training sessions</td>
<td></td>
<td></td>
<td>(134)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2) Provide a professional development/training programme for staff responsible for Information Lifecycle</td>
<td></td>
<td></td>
<td>(134)</td>
<td></td>
</tr>
<tr>
<td><strong>1</strong> Creation</td>
<td>1) Establish policy and procedure to guide and inform Staff on the best practice for creation of all types of information</td>
<td></td>
<td></td>
<td>(131)</td>
<td></td>
</tr>
</tbody>
</table>
| | 2) Establish procedures to ensure:  
   - Legal and Statutory Requirements are met  
   - New types of information have a lifecycle determined at the point of creation  
   - Any access restrictions are also determined at the point of creation | | | (131) | |
| **2** Retention | 1) Ensure CCG consistent adherence with the Records Management Code of Practice | | | | |
| | 2) Establish procedures for the closure of information when no longer current, including:  
   - Secure Storage of archived information | | | (346) | |
<table>
<thead>
<tr>
<th>Secure Storage of information awaiting disposal</th>
<th>Effective Disposal as soon as appropriate</th>
</tr>
</thead>
<tbody>
<tr>
<td>(C) Organise appropriate storage for active information including:</td>
<td>(347)</td>
</tr>
<tr>
<td>● Secure from flood, fire and theft</td>
<td></td>
</tr>
<tr>
<td>● Secure from unauthorised access</td>
<td></td>
</tr>
<tr>
<td>● 'Back up' systems</td>
<td></td>
</tr>
<tr>
<td>● Unauthorised alterations</td>
<td></td>
</tr>
<tr>
<td>● accidental erasure</td>
<td></td>
</tr>
</tbody>
</table>

| (3) Maintenance | (A) Develop, Implement and test disaster recovery plan for Key CCG information needed to function in the event of a failure, ensuring appropriate protection is in place for all | (346) |
| B) Allocate CCG wide resources to enable the continued implementation and maintenance of Information and to support the records management function | |
| (C) Review/Audit existing practices to establish compliance with the Records Management Code of Practice. | |

<p>| (4) Use | (A) The use of 100% verified NHS number for active electronic records and all patient communications | (421) |
| B) For scanned information the adoption of the BSI publication BIP 0008:2004 Code of Practice for legal admissibility and evidential weight of information stored electronically | |
| C) Develop Strategy to | (131) |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>reduce duplication and to aid information sharing, reduced costs and save space</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(D) Establish KPI's to assist performance against the Strategy and complete and audit (e.g responses to SARS/FOIR's/ Record Keeping, Availability etc)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| (E) Implement effective tracking systems and tracing audit trails, ensuring that information:  
  • Can be retrieved efficiently when required  
  • Is securely stored whilst still allowing necessary access to authorised personnel |   |   |   |
| (F) Develop and Ensure that standards for safe and secure transportation of paper information are consistently and strictly applied. |   |   |   |
| (G) Develop Strategy to improve quality, Check compliance and monitor effectiveness |   |   |   |
| (H) Develop appropriate Information Sharing protocols and subject specific information sharing agreements for the exchanges of Person Identifiable data |   |   |   |
| (I) Provide Guidance on back up archiving processing and audit trail for electronic records as well as on measure to prolong their access and use. For as long as required, including migration across systems and onto different types of media |   |   |   |
| (J) Update and improve the document template for widespread CCG usage. Ensure template is:  
  • Approved by the |   |   |   |
### (5) Disposal

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>(A) Establish the secure and confidential method to be used for the disposal of information and organise its implementation. (Approved contractor or by Cross Cut shredders to the DIN specification of Level 3 or above). Consider and include disposal of electronic held information as well as paper. Ensure adherence to the retention schedules.</td>
<td></td>
<td></td>
<td></td>
<td>NA</td>
</tr>
<tr>
<td>(B) Create and maintain a log of destroyed information, include:</td>
<td></td>
<td></td>
<td></td>
<td>NA</td>
</tr>
<tr>
<td>- Unique reference</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Description</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Date of destruction</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Destruction decisions</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Risk assessment of disposal (consider impacts of not disposing and/or delaying disposal).</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Appendix B: Rules of File-Naming

Rule 1: Keep file names short, but meaningful
File names should be kept as short as possible whilst also being meaningful. Long file names mean long file paths and long URLs which increase the likelihood of error, are more difficult to remember and recognise, and are more difficult to transmit in emails as they often ‘break’. However, avoid using initials, abbreviations and codes that are not commonly understood.

Rule 1 Example
Incorrect – The_long_and_short_committe_remit.rtf
Correct – LongShortCtteeRemit.rtf

Explanation Some words add length to a file name but do not contribute towards the meaning, for example words like “the”, “a”, and “and”. Where the remaining file name is still meaningful within the context of the file directory these elements can be removed. Sometimes words have standard abbreviations, e.g. ‘cttee’ is a standard abbreviation for “committee”; where this is the case the standard abbreviation can be used.

Rule 2: Avoid unnecessary repetition and redundancy in file names and file paths
Avoid redundancy in file names and file paths. Unnecessary repetition increases the length of file names and file paths, which is incompatible with Rule 1.

Rule 2 Examples
Incorrect - /../Court/20041030CourtMinutes.rtf
Correct - /../Court/20041030Minutes.rtf
Incorrect - /../Procedures/AppealsProcedures.rtf
Correct - /../Procedures/Appeals.rtf

Explanation In the first example the folder is called “Court” so it is not necessary to include the word “Court” in the file name because all the records in that folder are Court records.
In the second example the folder is called ‘Procedures’ so it is not necessary to include the word ‘Procedures’ in the file name because all the records in that folder are procedure records.

Rule 3: Use capital letters to delimit words, not spaces or underscores
Avoid using spaces and underscores in file names. Some software packages have difficulty recognising file names with spaces, this can be a particular difficulty for files when they are published on an external website, so it is best to avoid using spaces. Using underscores and hyphens in your file names increases the length, which is incompatible with Rule 1.
Where capitalised acronyms are used in file names the acronym should appear in capitals and the first letter of the following word should also be capitalised.
Rule 3 Example
Incorrect – RAE_instructions.html
Correct – RAEInstructions.html

Explanation Removing the space or underscore reduces the length of the file name, but by using capital letters to differentiate between the words the file name is still readily recognisable.

Rule 4: When including a number in a file name always give it as a two-digit number, unless it is a year or another number with more than two digits
The file directory displays file names in alphanumeric order. To maintain the numeric order when file names include numbers it is important to include the zero for numbers 0-9. This helps to retrieve the latest record number.

Rule 4 Example
Incorrect -
OfficeProceduresV1
OfficeProceduresV11
OfficeProceduresV2
OfficeProceduresV3

Correct –
OfficeProceduresV01
OfficeProceduresV02
OfficeProceduresV03
OfficeProceduresV04

Explanation This example shows the successive versions of an office procedures document. If two-digit numbers are used the latest version will always be at the bottom of the list.

Rule 5: 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:
YYYYMMDD or YYYYMM or YYYY or YYYY-YYYY
Dates should always be presented ‘back to front’, that is with the year first (always given as a four digit number), followed by the month (always given as a two digit number), and the day (always given as a two digit number). Using the dates back to front means that the chronological order of the records is maintained when the file names are listed in the file directory. This helps when trying to retrieve the latest dated record.

Rule 5 Example
Incorrect -
1Feb2005Agenda.rtf
1Feb2005Minutes.rtf
Explanation This example shows the minutes and papers of a committee. By stating the year 'back to front' the minutes and papers from the most recent meeting appear at the bottom of the directory list.

**Rule 6: In limited circumstances it may be appropriate to include a personal name in a file name give the family name first followed by the initials**

It may be appropriate to include within a file name the name of an individual, usually when the record is a piece of correspondence. However, it will not usually be appropriate to name records after the record owner or creator, i.e. avoid naming records after yourself or the person you work for. When it is appropriate to include a personal name it should be given as family name first followed by initials as it is most likely that the record will be retrieved according to the family name of the individual. Take care to ensure that no breach of confidentiality occurs in these circumstances e.g. save in a password protected folder.

**Rule 6 Example**

**Incorrect** - SamRBrown20041201.rtf  
**Correct** - BrownSR20041201.rtf

Explanation This is a letter to Mr Samuel R Brown. By putting the family name first the file directory will display this file next to the b’s, which is where you would expect to find a letter to Mr Brown.

**Rule 7: Avoid using common words such as ‘draft’ or ‘letter’ at the start of file names**

Avoid using common words such as ‘draft’ or ‘letter’ at the start of file names, or all of those records will appear together in the file directory, making it more difficult to retrieve the records you are looking for. This rule can be ignored if starting file names with these sorts of words aids the retrieval of the records. See rule 8 for further details.

**Rule 7 Example**

**Incorrect** -  
/…/Publicity/DraftAdvertising.rtf  
/…/Publicity/DraftOfficeProcedures.rtf  
/…/Publicity/FinalAdvertising.rtf
Explanation
The file directory will list files in alphanumeric order. This means that all records with file names starting “Draft” will be listed together. When retrieving files it will be more useful to find the draft budget report next to the previous year’s budget, rather than next to an unrelated draft record.

Rule 8: Order the elements in a file name in the most appropriate way to retrieve the record
The elements to be included in a file name should be ordered according to the way in which the record will be retrieved during the course of everyday business. This will depend on the way you work. For example, if the records are retrieved according to their date, the date element should appear first. If the records are retrieved according to their description, the description element should appear first.

Rule 8 Example
Incorrect
/…/OatcakeCttee/Agenda1Feb2005.rtf
/…/OatcakeCttee/Agenda20Jan2005.rtf
/…/OatcakeCttee/Agenda30June2004.rtf
/…/OatcakeCttee/Minutes1Feb2005.rtf
/…/OatcakeCttee/Minutes20Jan2005.rtf
/…/OatcakeCttee/Minutes30June2004.rtf
/…/Events/20030304WeddingDinner.rtf
/…/Events/20040630GardenParty.rtf
/…/Events/20040905ProcurementAward.rtf

Correct –
/…/OatcakeCttee/20040630Agenda.rtf
/…/OatcakeCttee/20040630Minutes.rtf
/…/OatcakeCttee/20050120Agenda.rtf
/…/OatcakeCttee/20050120Minutes.rtf
/…/OatcakeCttee/20050201Agenda.rtf
/…/OatcakeCttee/20050201Minutes.rtf
/…/Events/GardenParty20040630.rtf
/…/Events/ProcurementAward20040905.rtf
/…/Events/WeddingDinner20030304.rtf
Explanation The first example shows minutes and agenda of the Oatcake Committee. Minutes and papers of a meeting are likely to be retrieved on the basis of the date of the meeting, it is therefore best to have the date at the start of the file name, otherwise all the Agendas will come at the top of the directory list, followed by all of the minutes, and then by the papers.

The second example shows the file names of the files in the Events folder. Because events are likely to be retrieved by the name of the event rather than the date of the event, it is most useful to have that element first.

Rule 9: The file names of records relating to recurring events should include the date and a description of the event, except where the inclusion of either of these elements would be incompatible with Rule 2

The file names of records relating to recurring events (e.g. meeting minutes and papers, weekly, monthly or annual reports, event management and budget planning documents) should include both the date and the event name or event description so that the record can be identified and retrieved.

When deciding the order of the elements consider rule 8. Date first will usually be appropriate for events that are time specific and recurring. Event first will usually be appropriate for events that are infrequent, but regularly recurring. The event description could be the title of the event or the subject of the event, whatever description you choose, ensure that it is short, to the point, and readily recognisable to you and the colleagues you work with.

Rule 9 Example
Incorrect
/…/Website/WebStats20040301.rtf
/…/Website/WebStats20040401.rtf
/…/Planning/2003-2004BudgetV10.xls
/…/Planning/2004-2005BudgetV01Draft.xls
Correct –
/…/Website/20040301WebStats.rtf
/…/Website/20040401WebStats.rtf
/…/Planning/Budget2003-2004V10.xls
/…/Planning/Budget2004-2005V01Draft.xls

Explanation The first example shows the website statistic reports which are created on a monthly basis. Because the reports recur frequently and are retrieved by date it is most appropriate that the date is given first. Also remember Rule 2; in some cases it may be appropriate for the folder to be called ‘WebStats’, in which case the file names only need to include the date. For another example see the first Rule 8 example.

The second example shows annual budget reports. Because the reports are annual and likely to be retrieved by the description rather than the date, it is likely that it will be most appropriate for the description element to come first. Also remember Rule 2; in some cases it may be appropriate for the folder to be called “Planning2003-2004”, in which case the file names only need to include a description. For another example see the second Rule 8 example.
Rule 10: 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 Rule 2

The file names of correspondence should include the following elements so that the record can be easily identified and retrieved:

- Name of correspondent, that is the either the name of the person who sent you the letter/email/memo or the name of the person to whom you sent the letter/email/memo
- Subject description, where it is not given in the folder title
- Date of letter/email/memo
- If incoming correspondence, include ‘rcvd’

When deciding the order of the elements consider Rule 8. It will usually be appropriate to order the elements in the same order in which they are listed above, as it is likely that correspondence will be retrieved on the basis of the correspondent. Also consider Rule 2; a description of the subject may already be given in the folder name.

Rule 10 Example
Incorrect
/…/Complaints/EmailFromHelenThomas10Jun03.txt
/…/Complaints/LetterFromJoeBloggs5Jan04.rtf
/…/Complaints/LetterToHelenThomas10Jul03.rtf
/…/Complaints/LetterToJoeBloggs20Feb04.rtf
/…/Complaints/LetterToJoeBloggs5Dec03.rtf

Correct –
/…/Complaints/BloggsJ20031205.rtf
/…/Complaints/BloggsJ20040105rcvd.rtf
/…/Complaints/BloggsJ20040220.rtf
/…/Complaints/ThomasH20030610rcvd.txt
/…/Complaints/ThomasH20030710.rtf

Explanation The example shows some incoming and outgoing correspondence concerning complaints. All the correspondence with Mr Joe Bloggs appears together in chronological order and it is easy to pick out the incoming correspondence because it is indicated by ‘rcvd’. The same is true of the correspondence with Miss Helen Thomas. In this example it is not necessary to include an indication of the subject in the file name because it is given in the folder name.
Rule 11: The version number of a record should be indicated in its file name by the inclusion of ‘V’ followed the version number and, where applicable, ‘Draft’ or ‘Final’.

Some records go through a number of versions, for example they start out as working drafts, become consultation drafts and finish with a final draft, which may then be reviewed and updated at a later date. It is important to be able to differentiate between these various drafts by giving them each their own number. Where a version number is applicable, it should always appear in the file name of the record so that the most recent version can be easily identified and retrieved.

Rule 11 Example
Incorrect
Iemodel0304_draftv3.htm
Iemodle0304_finalv4htm
Org_Hier_2002_v2.xls
Org_Hier_2002_v3.xls
Org_Hier_2002_v4.xls

Correct –
IEAM2003-2004V03Draft.htm
IEAM2003-2004V04Final.htm
OrgHier2002V02.xls
OrgHier2002V03.xls
OrgHier2002V04.xls

Explanation The first example shows two versions of the income and expenditure attribution model for 2003-2004, version 3 is a draft version and version 4 is the final version. The common abbreviation for the model is used. The covering years are given in four-digit format. The version number is given with two digits so that the versions will appear in numeric order.

The second example shows a number of versions of the organisational hierarchy for 2002. In this case none of the versions are marked as draft or final because the nature of the record means that ‘draft’ and ‘final’ are not applicable.
Appendix C: Flowchart to Determine if Emails Have Value

1. Does the e-mail contain information which is related to work? 
   - NO: E-mail is personal and not a record.
   - YES: Are you the only recipient of this e-mail?

2. Are you the only recipient of this e-mail? 
   - NO: Did you send the e-mail? 
     - NO: Was the e-mail cc’d to you? 
       - NO: Was the e-mail sent to a discussion list or listserv? 
         - YES: The e-mail should not be managed as a record.
         - NO: The e-mail is a corporate record.
   - YES: Manage the other source of information as the record.

3. Is the e-mail the primary source of this information? 
   - NO: Will the e-mail contain information that will be used as a basis for future decisions? 
     - NO: Does the e-mail contain information which is related to work? 
       - NO: E-mail is not a corporate record.
       - YES: The e-mail is a corporate record.
     - YES: Does the e-mail require or authorise an important course of action? 
       - NO: Does the e-mail protect rights, assets or other rights of the Trust or its stakeholders?
       - YES: The e-mail is a corporate record.
   - YES: Could this e-mail be used to provide evidence of a business activity or transaction? 
     - NO: Does the e-mail detail any liabilities or responsibilities of the Trust? 
       - NO: Does the e-mail require or authorise an important course of action? 
         - NO: Does the e-mail protect rights, assets or other rights of the Trust or its stakeholders?
         - YES: The e-mail is a corporate record.
       - YES: The e-mail is not a corporate record.
Appendix D: Classification of NHS Information – Marking Guidance

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

**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.

### Table 1 – Descriptors that may be used with “NHS CONFIDENTIAL” or “NHS PROTECT” marking

<table>
<thead>
<tr>
<th>Category</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appointments</td>
<td>Concerning actual or potential appointments not yet announced.</td>
</tr>
</tbody>
</table>
| 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                                                                                                                                                            |
Appendix E: Legal Acts Pertaining to this Document

- **The Data Protection Act 1998**: all staff must abide by the Data Protection Act 1998. Personal information relating to staff, suppliers, etc may only be accessed and used by staff on a need to know basis. Unauthorised disclosure of such "personal data" may result in disciplinary action and prosecution. Under the Act personal data must be:
  - obtained and processed fairly and lawfully;
  - processed for limited purpose;
  - adequate, relevant and not excessive;
  - accurate;
  - kept no longer than necessary;
  - processed in line with the rights of the data subject;
  - secure;
  - not transferred to countries outside of the EEA unless they offer adequate protection.

Every individual, including staff, is entitled to be informed of any personal data held on them by the organisation, to access that data and to have it corrected if it is inaccurate. All enquiries relating to the Data Protection Act must be referred to the Data Protection Officer.


- **The Copyright, Designs and Patents Act 1988**: It is illegal to copy, without the appropriate consent, software except for backup purposes, and each machine must have a license for its software. The copyright owner has the right to bring civil proceedings and in certain circumstances criminal proceedings against those that infringe their rights.

- **Department of Health Guidance**: Guidance and standards for the Protection and Use of Patient Information and Caldicott Guardian guidance can be found on the Department of Health website.
## Appendix F: Clinical Record Retention Periods

<table>
<thead>
<tr>
<th>Type of Record (Clinical)</th>
<th>Retention Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>A&amp;E Records</td>
<td>8 years adult, 25th birthday child</td>
</tr>
<tr>
<td>Admission Books</td>
<td>8 years</td>
</tr>
<tr>
<td>Ambulance Records</td>
<td>10 years</td>
</tr>
<tr>
<td>Audiology Records</td>
<td>8 years adult, 25th birthday child</td>
</tr>
<tr>
<td>Birth Registers</td>
<td>2 years</td>
</tr>
<tr>
<td>Birth Notification</td>
<td>25th birthday of child</td>
</tr>
<tr>
<td>Cancer Care Records</td>
<td>8 years adult, 25th birthday child</td>
</tr>
<tr>
<td>Child Health Record</td>
<td>25th birthday of child</td>
</tr>
<tr>
<td>Clinical Audit Records</td>
<td>5 years</td>
</tr>
<tr>
<td>Clinical Psychology</td>
<td>20 years</td>
</tr>
<tr>
<td>Death Registers</td>
<td>2 years</td>
</tr>
<tr>
<td>Dental Records Including Study Models</td>
<td>11 years adult, 25th birthday child</td>
</tr>
<tr>
<td>Diaries</td>
<td>2 years after current year</td>
</tr>
<tr>
<td>Dietetic and Nutrition</td>
<td>8 years adult, 25th birthday child</td>
</tr>
<tr>
<td>District Nurse Records</td>
<td>8 years adult, 25th birthday child</td>
</tr>
<tr>
<td>DNA (Did Not Attend)</td>
<td>8 years adult, 25th birthday child</td>
</tr>
<tr>
<td>Electrocardiogram (ECG) Records</td>
<td>7 years</td>
</tr>
<tr>
<td>Endoscopy Records</td>
<td>8 years adult, 25th birthday child</td>
</tr>
<tr>
<td>Family Planning Records</td>
<td>10 years adult, 25th birthday child</td>
</tr>
<tr>
<td>GP Records</td>
<td>10 years after death or emigration</td>
</tr>
<tr>
<td>Health Visitor Records</td>
<td>10 years</td>
</tr>
<tr>
<td>Hospital Acquired Infection Records</td>
<td>6 years</td>
</tr>
<tr>
<td>Hospital Records Not Listed Elsewhere</td>
<td>8 years after treatment</td>
</tr>
<tr>
<td>Immunisation and Vaccination Records</td>
<td>10 years</td>
</tr>
<tr>
<td>Joint Replacement Records</td>
<td>10 years</td>
</tr>
<tr>
<td>Learning Disabilities (Adult)</td>
<td>20 years, or 8 years if died in care</td>
</tr>
<tr>
<td>Learning Disabilities (Child)</td>
<td>25th birthday</td>
</tr>
<tr>
<td>Maternity, Midwifery and Neonatal</td>
<td>25 years after birth of last child</td>
</tr>
<tr>
<td>Mentally Disordered Persons (Adult)</td>
<td>20 years, or 8 years if died in care</td>
</tr>
<tr>
<td>Mentally Disordered Persons (Child)</td>
<td>20 years or 25th birthday if longer</td>
</tr>
<tr>
<td>Neonatal Screening Records</td>
<td>25 years</td>
</tr>
<tr>
<td>Nicotine Replacement Therapy (Stop Smoking)</td>
<td>2 years</td>
</tr>
<tr>
<td>Occupational Health Records (Staff)</td>
<td>3 years after employment termination</td>
</tr>
<tr>
<td>Occupational Related Diseases (e.g. Asbestosis)</td>
<td>10 years</td>
</tr>
<tr>
<td>Occupational Therapy</td>
<td>8 years adult, 25th birthday child</td>
</tr>
<tr>
<td>Oncology, Radiotherapy</td>
<td>30 years</td>
</tr>
<tr>
<td>Operating Theatre Lists</td>
<td>4 years</td>
</tr>
<tr>
<td>Operating Theatre Registers</td>
<td>8 years</td>
</tr>
<tr>
<td>Orthoptic Records</td>
<td>8 years adult, 25th birthday child</td>
</tr>
<tr>
<td>Outpatient Lists</td>
<td>2 years after current year</td>
</tr>
<tr>
<td>Parent-Held Records</td>
<td>Retrieve, then retain as per record type</td>
</tr>
<tr>
<td>Patient-Held Records</td>
<td>Retrieve, then retain as per record type</td>
</tr>
<tr>
<td>Physiotherapy Records</td>
<td>8 years adult, 25th birthday child</td>
</tr>
<tr>
<td>Podiatry Records</td>
<td>8 years adult, 25th birthday child</td>
</tr>
<tr>
<td>Prescriptions</td>
<td>2 years</td>
</tr>
<tr>
<td>Psychotherapy Records</td>
<td>20 years, or 8 years if died in care</td>
</tr>
<tr>
<td>Litigation Records</td>
<td>As advised by Legal Dept</td>
</tr>
<tr>
<td>Records of Destruction of Health Records</td>
<td>Permanently</td>
</tr>
<tr>
<td>Recovery Room Records</td>
<td>8 years</td>
</tr>
<tr>
<td>Referral Letters</td>
<td>8 years adult, 25th birthday child</td>
</tr>
<tr>
<td>Scanned Records</td>
<td>As per record type</td>
</tr>
<tr>
<td>Speech and Language Therapy</td>
<td>8 years adult, 25th birthday child</td>
</tr>
<tr>
<td>X-Ray Films</td>
<td>8 years adult, 25th birthday child</td>
</tr>
</tbody>
</table>
## Appendix G: Corporate Record Retention Periods

<table>
<thead>
<tr>
<th>Type of Record (Corporate)</th>
<th>Retention Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accident Records</td>
<td>10 years</td>
</tr>
<tr>
<td>Agendas (Board Meetings and Major Committees)</td>
<td>30 years</td>
</tr>
<tr>
<td>Agendas (Other)</td>
<td>2 years</td>
</tr>
<tr>
<td>Audit Records (Internal and External)</td>
<td>2 years from completion of audit</td>
</tr>
<tr>
<td>Business and Local Delivery Plans</td>
<td>20 years</td>
</tr>
<tr>
<td>CCTV Images</td>
<td>31 days</td>
</tr>
<tr>
<td>Commissioning Decisions and Appeals</td>
<td>6 years</td>
</tr>
<tr>
<td>Complaints Documentation</td>
<td>8 years</td>
</tr>
<tr>
<td>Data Protection Act Requests</td>
<td>3 years</td>
</tr>
<tr>
<td>Freedom of Information Act Requests</td>
<td>3 years, 10 years if withheld</td>
</tr>
<tr>
<td>Health &amp; Safety Documentation</td>
<td>3 years</td>
</tr>
<tr>
<td>Incident Forms</td>
<td>10 years</td>
</tr>
<tr>
<td>Litigation</td>
<td>10 years or as advised by Legal Dept</td>
</tr>
<tr>
<td>Meeting &amp; Minute Papers (Major Committees incl. Board)</td>
<td>30 years</td>
</tr>
<tr>
<td>Meeting &amp; Minute Papers (Other Committees)</td>
<td>2 years</td>
</tr>
<tr>
<td>Mortgage Documents (Acquisition, Transfer, Disposal)</td>
<td>6 years after repayment</td>
</tr>
<tr>
<td>PALS Records</td>
<td>10 years</td>
</tr>
<tr>
<td>Papers of Minor or Brief Importance Not Covered Elsewhere</td>
<td>2 years</td>
</tr>
<tr>
<td>Patient Surveys</td>
<td>2 years</td>
</tr>
<tr>
<td>Project Files</td>
<td>6 years</td>
</tr>
<tr>
<td>Public Consultations</td>
<td>5 years</td>
</tr>
<tr>
<td>Quality &amp; Outcomes Framework (QOF) Documents</td>
<td>2 years</td>
</tr>
<tr>
<td>Reports</td>
<td>30 years</td>
</tr>
<tr>
<td>Requisitions</td>
<td>18 months</td>
</tr>
<tr>
<td>Research Ethics Committee Records</td>
<td>3 years from date of decision</td>
</tr>
<tr>
<td>Serious Incident / Serious Untoward Incident (SUI) Files</td>
<td>30 years</td>
</tr>
<tr>
<td>Statistics</td>
<td>3 years</td>
</tr>
<tr>
<td>Timesheets</td>
<td>2 years</td>
</tr>
<tr>
<td>Building &amp; Engineering Works</td>
<td>30 years</td>
</tr>
<tr>
<td>Building Plans, Deeds, Drawings &amp; Records</td>
<td>Lifetime of building</td>
</tr>
<tr>
<td>Inspection Reports</td>
<td>Lifetime of Installation</td>
</tr>
<tr>
<td>Maintenance Contracts</td>
<td>6 years from end of contract</td>
</tr>
<tr>
<td>Manuals</td>
<td>Lifetime of equipment</td>
</tr>
<tr>
<td>Medical Device Alerts</td>
<td>Until updated or withdrawn</td>
</tr>
<tr>
<td>Accounts – Annual (Final)</td>
<td>30 years</td>
</tr>
<tr>
<td>Accounts – Receipts, Slips, Counterfoils, Vouchers etc.</td>
<td>2 years</td>
</tr>
<tr>
<td>BACS Records</td>
<td>6 years after current year</td>
</tr>
<tr>
<td>Contracts</td>
<td>15 years</td>
</tr>
<tr>
<td>Creditor Records</td>
<td>3 years after current year</td>
</tr>
<tr>
<td>Debtor Records</td>
<td>6 years after current year</td>
</tr>
<tr>
<td>Documents Not Mentioned Elsewhere</td>
<td>6 years</td>
</tr>
<tr>
<td>Expense Claims</td>
<td>5 years after current year</td>
</tr>
<tr>
<td>Fraud Case Files</td>
<td>6 years after current year</td>
</tr>
<tr>
<td>General Medical Services Payments</td>
<td>6 years after current year</td>
</tr>
<tr>
<td>Invoices, Ledgers, Journals, VAT Records, Bills</td>
<td>6 years after current year</td>
</tr>
<tr>
<td>PAYE Records</td>
<td>6 years after employment termination</td>
</tr>
<tr>
<td>Payroll</td>
<td>6 years after current year</td>
</tr>
<tr>
<td>HR Records (Main Record)</td>
<td>6 years after individual leaves</td>
</tr>
<tr>
<td>HR Records (Summary of Record)</td>
<td>Until individuals 70th Birthday</td>
</tr>
<tr>
<td>IM&amp;T Software Licenses</td>
<td>Lifetime of software</td>
</tr>
<tr>
<td>Job Applications (Successful)</td>
<td>3 years after employment termination</td>
</tr>
<tr>
<td>Job Applications (Unsuccessful)</td>
<td>1 year</td>
</tr>
<tr>
<td>Leaver’s Dossiers</td>
<td>6 years after employment termination</td>
</tr>
<tr>
<td>Personnel / HR Records</td>
<td>6 years after employment termination</td>
</tr>
<tr>
<td>Study Leave Applications</td>
<td>5 years</td>
</tr>
<tr>
<td>Timesheets</td>
<td>2 years after current year</td>
</tr>
<tr>
<td>Tenders (successful)</td>
<td>Tender period plus 6 years</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Tenders (unsuccessful)</td>
<td>6 years</td>
</tr>
</tbody>
</table>
Appendix H: Process Map for Scanning a Document Received Via Post

Start → Document received via post → Document date stamped → Document scanned

Trouble shoot the problem and scan image again.

Is the document a true representation of the original document?

Yes → Can you read the document?

Yes → Is it clear who the document is concerning?

Yes → Is the date stamp clear?

Yes → Save the document in the system → Stop

No → Can you read the document?

Yes → Is it clear who the document is concerning?

Yes → Is the date stamp clear?

Yes → Save the document in the system → Stop

No → Can you read the document?

Yes → Is it clear who the document is concerning?

Yes → Is the date stamp clear?

Yes → Save the document in the system → Stop

No → Can you read the document?

Yes → Is it clear who the document is concerning?

Yes → Is the date stamp clear?

Yes → Save the document in the system → Stop

No → Can you read the document?

Yes → Is it clear who the document is concerning?

Yes → Is the date stamp clear?

Yes → Save the document in the system → Stop

No → Can you read the document?

Yes → Is it clear who the document is concerning?

Yes → Is the date stamp clear?

Yes → Save the document in the system → Stop

No → Can you read the document?

Yes → Is it clear who the document is concerning?

Yes → Is the date stamp clear?

Yes → Save the document in the system → Stop

No → Can you read the document?

Yes → Is it clear who the document is concerning?

Yes → Is the date stamp clear?

Yes → Save the document in the system → Stop

No → Can you read the document?

Yes → Is it clear who the document is concerning?

Yes → Is the date stamp clear?

Yes → Save the document in the system → Stop

No → Can you read the document?

Yes → Is it clear who the document is concerning?

Yes → Is the date stamp clear?

Yes → Save the document in the system → Stop

No → Can you read the document?

Yes → Is it clear who the document is concerning?

Yes → Is the date stamp clear?

Yes → Save the document in the system → Stop

No → Can you read the document?

Yes → Is it clear who the document is concerning?

Yes → Is the date stamp clear?

Yes → Save the document in the system → Stop

No → Can you read the document?

Yes → Is it clear who the document is concerning?

Yes → Is the date stamp clear?

Yes → Save the document in the system → Stop

No → Can you read the document?

Yes → Is it clear who the document is concerning?

Yes → Is the date stamp clear?

Yes → Save the document in the system → Stop

No → Can you read the document?

Yes → Is it clear who the document is concerning?

Yes → Is the date stamp clear?

Yes → Save the document in the system → Stop

No → Can you read the document?

Yes → Is it clear who the document is concerning?

Yes → Is the date stamp clear?

Yes → Save the document in the system → Stop

No → Can you read the document?

Yes → Is it clear who the document is concerning?

Yes → Is the date stamp clear?

Yes → Save the document in the system → Stop

No → Can you read the document?

Yes → Is it clear who the document is concerning?

Yes → Is the date stamp clear?

Yes → Save the document in the system → Stop

No → Can you read the document?

Yes → Is it clear who the document is concerning?

Yes → Is the date stamp clear?

Yes → Save the document in the system → Stop

No → Can you read the document?

Yes → Is it clear who the document is concerning?

Yes → Is the date stamp clear?

Yes → Save the document in the system → Stop

No → Can you read the document?

Yes → Is it clear who the document is concerning?

Yes → Is the date stamp clear?

Yes → Save the document in the system → Stop

No → Can you read the document?

Yes → Is it clear who the document is concerning?

Yes → Is the date stamp clear?

Yes → Save the document in the system → Stop

No → Can you read the document?

Yes → Is it clear who the document is concerning?

Yes → Is the date stamp clear?

Yes → Save the document in the system → Stop

No → Can you read the document?

Yes → Is it clear who the document is concerning?

Yes → Is the date stamp clear?

Yes → Save the document in the system → Stop

No → Can you read the document?

Yes → Is it clear who the document is concerning?

Yes → Is the date stamp clear?

Yes → Save the document in the system → Stop

No → Can you read the document?

Yes → Is it clear who the document is concerning?

Yes → Is the date stamp clear?

Yes → Save the document in the system → Stop

No → Can you read the document?

Yes → Is it clear who the document is concerning?

Yes → Is the date stamp clear?

Yes → Save the document in the system → Stop

No → Can you read the document?

Yes → Is it clear who the document is concerning?

Yes → Is the date stamp clear?

Yes → Save the document in the system → Stop

No → Can you read the document?

Yes → Is it clear who the document is concerning?

Yes → Is the date stamp clear?

Yes → Save the document in the system → Stop

No → Can you read the document?

Yes → Is it clear who the document is concerning?

Yes → Is the date stamp clear?

Yes → Save the document in the system → Stop

No → Can you read the document?

Yes → Is it clear who the document is concerning?

Yes → Is the date stamp clear?

Yes → Save the document in the system → Stop

No → Can you read the document?

Yes → Is it clear who the document is concerning?

Yes → Is the date stamp clear?

Yes → Save the document in the system → Stop

No → Can you read the document?

Yes → Is it clear who the document is concerning?

Yes → Is the date stamp clear?

Yes → Save the document in the system → Stop

No → Can you read the document?

Yes → Is it clear who the document is concerning?

Yes → Is the date stamp clear?

Yes → Save the document in the system → Stop

No → Can you read the document?

Yes → Is it clear who the document is concerning?

Yes → Is the date stamp clear?

Yes → Save the document in the system → Stop

No → Can you read the document?

Yes → Is it clear who the document is concerning?

Yes → Is the date stamp clear?

Yes → Save the document in the system → Stop

No → Can you read the document?

Yes → Is it clear who the document is concerning?

Yes → Is the date stamp clear?

Yes → Save the document in the system → Stop

No → Can you read the document?

Yes → Is it clear who the document is concerning?

Yes → Is the date stamp clear?

Yes → Save the document in the system → Stop

No → Can you read the document?

Yes → Is it clear who the document is concerning?

Yes → Is the date stamp clear?

Yes → Save the document in the system → Stop

No → Can you read the document?

Yes → Is it clear who the document is concerning?

Yes → Is the date stamp clear?

Yes → Save the document in the system → Stop

No → Can you read the document?

Yes → Is it clear who the document is concerning?

Yes → Is the date stamp clear?

Yes → Save the document in the system → Stop

No → Can you read the document?

Yes → Is it clear who the document is concerning?

Yes → Is the date stamp clear?

Yes → Save the document in the system → Stop

No → Can you read the document?

Yes → Is it clear who the document is concerning?

Yes → Is the date stamp clear?

Yes → Save the document in the system → Stop

No → Can you read the document?

Yes → Is it clear who the document is concerning?

Yes → Is the date stamp clear?

Yes → Save the document in the system → Stop

No → Can you read the document?

Yes → Is it clear who the document is concerning?

Yes → Is the date stamp clear?

Yes → Save the document in the system → Stop

No → Can you read the document?

Yes → Is it clear who the document is concerning?

Yes → Is the date stamp clear?

Yes → Save the document in the system → Stop

No → Can you read the document?

Yes → Is it clear who the document is concerning?

Yes → Is the date stamp clear?

Yes → Save the document in the system → Stop

No → Can you read the document?

Yes → Is it clear who the document is concerning?

Yes → Is the date stamp clear?

Yes → Save the document in the system → Stop

No → Can you read the document?

Yes → Is it clear who the document is concerning?

Yes → Is the date stamp clear?

Yes → Save the document in the system → Stop

No → Can you read the document?

Yes → Is it clear who the document is concerning?

Yes → Is the date stamp clear?

Yes → Save the document in the system → Stop

No → Can you read the document?

Yes → Is it clear who the document is concerning?

Yes → Is the date stamp clear?

Yes → Save the document in the system → Stop

No → Can you read the document?

Yes → Is it clear who the document is concerning?

Yes → Is the date stamp clear?

Yes → Save the document in the system → Stop

No → Can you read the document?
## Checklist for Approval of Policy

To be completed and attached to any document which guides practice when submitted to the appropriate committee for consideration and approval.

<table>
<thead>
<tr>
<th>Title of document being reviewed:</th>
<th>Yes/No/Unsure</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1. Title</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is the title clear and unambiguous?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is it clear whether the document is a guideline, policy, protocol or standard?</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>2. Rationale</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are reasons for development of the document stated?</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>3. Development Process</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is the method described in brief?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are people involved in the development identified?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you feel a reasonable attempt has been made to ensure relevant expertise has been used?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is there evidence of consultation with stakeholders and users?</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>4. Content</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is the objective of the document clear?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is the target population clear and unambiguous?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are the intended outcomes described?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are the statements clear and unambiguous?</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>5. Evidence Base</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is the type of evidence to support the document identified explicitly?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are key references cited?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are the references cited in full?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are supporting documents referenced?</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>6. Approval</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does the document identify which committee/group will approve it?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Title of document being reviewed:</td>
<td>Yes/No/Unsure</td>
<td>Comments</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>---------------</td>
<td>----------</td>
</tr>
<tr>
<td>If appropriate have the joint Human Resources/staff side committee (or equivalent) approved the document?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

7. **Dissemination and Implementation**

Is there an outline/plan to identify how this will be done?

Does the plan include the necessary training/support to ensure compliance?

8. **Document Control**

Does the document identify where it will be held?

Have archiving arrangements for superseded documents been addressed?

9. **Process to Monitor Compliance and Effectiveness**

Are there measurable standards or KPIs to support the monitoring of compliance with and effectiveness of the document?

Is there a plan to review or audit compliance with the document?

10. **Review Date**

Is the review date identified?

Is the frequency of review identified? If so is it acceptable?

11. **Overall Responsibility for the Document**

Is it clear who will be responsible for co-ordinating the dissemination, implementation and review of the documentation?

12 **Equality Impact Assessment (EIA)**

Has an equality analysis been undertaken in preparation for this policy?

Has the equality analysis been quality assured by the Equality and Diversity Group?

**Individual Approval**

If you are happy to approve this document, please sign and date it and forward to the chair of the committee/group where it will receive final approval.

<table>
<thead>
<tr>
<th>Name</th>
<th>Date</th>
</tr>
</thead>
</table>

Signature
## Committee Approval

If the committee is happy to approve this document, please sign and date it and forward copies to the person with responsibility for disseminating and implementing the document and the person who is responsible for maintaining the organisation’s database of approved documents.

<table>
<thead>
<tr>
<th>Name</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Signature