Joint Policy for Cumbria Partnership Foundation Trust and North Cumbria University Hospital NHS Trust

Corporate Records Policy and Procedures (Joint)

Reference	POL/COR/001
Version	1.0
Date Ratified	09/08/2018
Next Review Date	September 2021
Accountable Director	Company Secretary
Policy Author	Head of Information Governance / Data Protection Officer

Please note that the Intranet / internet Policy web page version of this document is the only version that is maintained.

Any printed copies or copies held on any other web page should therefore be viewed as “uncontrolled” and as such, may not necessarily contain the latest updates and amendments.

Cumbria Partnership NHS Foundation Trust | North Cumbria University Hospitals NHS Trust

Policy On A Page

SUMMARY & AIM

The purpose of this policy is to set out the key principles which apply to the management of corporate records created, used, stored, archived and ultimately destroyed by Cumbria Partnership NHS Foundation Trust and North Cumbria University Hospitals (hereafter known as The Trust) and Organisations which under a Service Level Agreement receive Information Governance support and services from the Trust.

The policy has detailed procedural guidance at the back to follow also.

TARGET AUDIENCE:

All staff employed by the Trust(s), private contractors, volunteers and temporary staff.

TRAINING:

Mandatory Information Governance training.

Information asset owner / information asset administrator training

Training on the relevant information assets that are used.

KEY REQUIREMENTS

Understand the legal and professional obligations as to why you must follow this policy and procedure

Understand the principles to be followed.

Understand the process to be followed (in line with appendices which provides the procedures to follow)

Understand the vital records you hold and ensure that through excellent business continuity and disaster recovery that these are available.

Ensure compliance with the data security and protection toolkit and CQC (Care Quality Commission requirements)

TABLE OF CONTENTS

1. INTRODUCTION 4
2. PURPOSE 4
3. POLICY DETAILS 5
   - 3.1 Legal and Professional Obligations 5
   - 3.2 Principles 5
   - 3.3 Process 5
   - 3.3 Vital Records 6
   - 3.4 Business Continuity and Disaster Recovery 7
   - 3.5 Data Security and Protection Toolkit 7
4. TRAINING AND SUPPORT 7
5. PROCESS FOR MONITORING COMPLIANCE 7
6. REFERENCES: 7
7. ASSOCIATED DOCUMENTATION: 7
8. DUTIES (ROLES & RESPONSIBILITIES): 8
   - 8.1 Chief Executive / Trust Board Responsibilities: 8
   - 8.2 Executive Director Responsibilities: 8
   - 8.3 Managers Responsibilities: 8
   - 8.4 Staff Responsibilities: 8
   - 8.5 Approving Committee Responsibilities: 9
9. ABBREVIATIONS / DEFINITION OF TERMS USED 9

APPENDIX 1 – CORPORATE RECORDS PROCEDURES 10
   - a) General Principles 10
   - b) Records Creation 10
   - c) Records Keeping 10
   - d) Scanning 11
   - e) Record Maintenance 11
   - f) Access and DIsclosure 11
   - g) Closure and Transfer 12
   - h) Appraisal 12
   - i) Archive and Retention 12
   - j) Disposal 13
   - k) Corporate Records Audit – Annual Requirement 13

APPENDIX 2 – RECORDS CREATION GUIDANCE – FILING AND NAMING GUIDANCE 14

DOCUMENT CONTROL 21

1. INTRODUCTION

This policy relates to all non-clinical records held in any format by the Trust, it includes all administrative records in which any information created or received in the course of Trust business, which needs to be retained to provide evidence of a business activity, transaction or decision is recorded. These records can be known as Corporate Records.

Information is a corporate asset. The Trust's records are important sources of administrative, evidential and historical information. They are vital to the Trust to support its current and future operations (including meeting the requirements of Freedom of Information legislation), for the purpose of accountability, and for an awareness and understanding of its history and procedures.

2. PURPOSE

The purpose of this policy is to set out the key principles which apply to the management of corporate records created, used, stored, archived and ultimately destroyed by Cumbria Partnership NHS Foundation Trust and North Cumbria University Hospitals (hereafter known as The Trust) and Organisations which under a Service Level Agreement receive Information Governance support and services from the Trust

This policy is mandatory and applies to the management of all aspects of records whether internally or externally generated and in any format or media type.

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

The Management of Records is a prerequisite for the Trust as set out in Standing Orders (ref SFI19 Retention of Documents) which states:

"*All NHS records are public records under the terms of the Public Records Act 1958 section 3 (1) – (2). The Secretary of State for Health and all NHS organisations have a duty under this Act to make arrangements for the safe keeping and eventual disposal of all types of records. In addition, the requirements of the Data Protection Act 2018 and the Freedom of Information Act 2000 must be achieved."*

Implementation of this policy contributes to achievement of the Data Security and Protection Toolkit.

This policy will be applied to all staff groups regardless of gender, age, ethnicity, disability, marital status, sexual orientation, religion, faith or belief, socio-economic status or any other personal characteristic or situation.

3. POLICY DETAILS

3.1 Legal and Professional Obligations

All NHS records are Public Records under the Public Records Acts. The Trust will take actions as necessary to comply with the legal and professional obligations set out in the Records Management: NHS Code of Practice, in particular:

- The Public Records Act 1958;
- The Data Protection Act 2018;
- The Freedom of Information Act 2000;
- The Common Law Duty of Confidentiality and Code of Practice

And any new legislation affecting records management as it arises.

3.2 Principles

The Trust's records are its corporate memory, providing evidence of actions and decisions and representing a vital asset to support daily functions and operations. Records support policy formation and managerial decision-making, protect the interests of the Trust and the rights of patients, staff and members of the public. They support consistency, continuity, efficiency and productivity and help deliver services in consistent and equitable ways.

The Corporate Records Group via the Joint Information Governance (IG) Board has adopted this Corporate Records Policy and is committed to ongoing improvement of its records management functions as it believes that it will gain a number of organisational benefits from so doing. These include:

- better use of physical and server space;
- better use of staff time;
- improved control of valuable information resources;
- compliance with legislation and standards; and
- reduced costs.

It is, therefore, of paramount importance to ensure that all information is efficiently managed and that appropriate policies, procedures, management accountability and structures provide a robust governance framework for information management.

3.3 Process

The effective management of corporate records ensures that information is properly managed and is available whenever and wherever there is a justified need for that Information and in whatever media it is required.

Clear lines of responsibility and accountability will be established throughout the Trust to ensure that there is recognised structure for the management of Corporate Records.

A record can be in various formats including email, paper, digital, social media, videos and telephone messages.

All departments are responsible for their own records and will have individual operational procedures for their management .Operational Procedures will be based on the Corporate Records procedure and will clearly set out how Records are identified, filed, archived and destroyed.

Corporate Records are a vital asset and access should be controlled to protect this asset and ensure the integrity of the records is maintained.

Information Asset Owners will be recognised in all areas where records (assets) are created and managed. IAOs will work with IAAs to ensure that a robust system is in place to create and manage an inventory of records they own

Information Asset Owners will be responsible for ensuring that corporate records are catalogued in an Information Asset Store.

It is a policy goal that where possible records will be in electronic format. The use of paper records will gradually come to an end, thereby reducing costs and storage space.

For reasons such as business efficiency and to reduce storage space, paper documents may be scanned into electronic format and the paper version duly destroyed appropriately. Staff involved in scanning should understand the principles of information management encapsulated in Code of Practice BIP0008.

IAAs should be aware of the arrangements for archiving and accessing records at the contracted offsite storage depot - currently Fastness.

The National Archives is the body that is responsible for advising on the management of all types of public records, including NHS records. The National Archives has general oversight of the arrangements for the permanent preservation of records. Those Corporate Records identified for permanent preservation will be stored in the County Archives. A Register of records stored in the Archives will be maintained.

An annual audit of corporate records will be undertaken to identify

- the type of records currently held;
- the form in which they are held;
- the record keeping systems currently in use, how effective they are and those that need to be developed/updated/procured.

3.3 Vital Records

Vital records are those records without which an organisation could not continue to operate. They are the records which contain information needed to re-establish the business of the organisation in the event of a disaster or significant interruption to business and which protect the assets and interests of the organisation.

The Trust must protect its vital records by managing them within strict controls that protect their existence and accessibility. The Trust will ensure that the Asset register will identify which records are vital.

3.4 Business Continuity and Disaster Recovery

Vital Corporate Records are required to be included in the Trust's disaster recovery and business continuity plans

3.5 Data Security and Protection Toolkit

The Trust will work towards achieving requirements under CQC and the Data Security and Protection Toolkit.

4. TRAINING AND SUPPORT

- Completion of mandatory IG (information governance) training – annual
- Completion of IAO and IAA training – every three years for those with management responsibility
- All staff to ensure that they are competent in accessing the relevant information asset (i.e. sharepoint).

5. PROCESS FOR MONITORING COMPLIANCE

The process for monitoring compliance with the effectiveness of this policy is as follows:

Aspect being monitored	Monitoring Methodology	Reporting		
		Presented by	Committee	Frequency
Undertake an audit of Corporate Record Standards detailed in this policy .	Corporate Records Audit	Company Secretary	Corporate Records Group with results via Joint IG Board	Annual

6. REFERENCES:

Data Protection Act 2018
General Data Protection Regulations
Freedom of Information Act and Code of Practice
Code of Confidentiality and Common Law Duty of Confidentiality
Records Management Code of Practice

7. ASSOCIATED DOCUMENTATION:

Standing Orders, Reservations and Delegation of Powers and Standing Financial Instructions.

8. DUTIES (ROLES & RESPONSIBILITIES):

8.1 Chief Executive / Trust Board Responsibilities:

The Chief Executive and Trust Board jointly have overall responsibility for the strategic and operational management of the Trust, including ensuring that Trust policies comply with all legal, statutory and good practice requirements.

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

8.2 Executive Director Responsibilities:

All policies have a designated Executive Director and it is their responsibility to be involved in the development and sign off of the policies, this should ensure that Trust policies meet statutory legislation and guidance where appropriate. They must ensure the policies are kept up to date by the relevant author and approved at the appropriate committee.

Senior Information Risk Owner - The SIRO is an executive Board member with allocated lead responsibility for the Trust's information risks and provides a focus for the management of information risk at Board level.

Joint Company Secretary - The Joint Company Secretary will hold management accountability and has a role to encourage services in the Trust to meet the required standards for Corporate Records.

8.3 Managers Responsibilities:

Information Asset Owners - The Information Asset Owner (IAO) is a senior member of staff who is the nominated owner for one or more identified information assets of the organisation. Their role is to understand and address risks to the information assets they 'own' and to provide assurance to the SIRO on the security and use of those assets.

Information Asset Administrators - Information Asset Administrators ensure that policies and procedures are followed, recognise actual or potential security incidents, consult their IAO on incident management, and ensure that information asset registers are accurate and up to date.

Head of Information Governance - Head of Information Governance is responsible for ensuring the organisation meets its statutory and corporate responsibilities and engender trust from the public in the management of their personal information.

8.4 Staff Responsibilities:

All Trust employees and anyone else working for the organisation (eg. Agency staff, honorary contracts, management consultants etc) who use and have access to Trust information must ensure that they are fully aware of their responsibilities in respect of record keeping and management. Under the Public Record Act, all NHS employees have a degree of responsibility for any records that they create or use. Thus, any records created by an employee of the NHS are public records and may be subject to both legal and professional obligations.

8.5 Approving Committee Responsibilities:

The Chair of the approving committee will ensure the policy approval is documented in the final section of the Checklist for Policy Changes. The committee will agree the approval of the final draft of the policy.

The Corporate Records Group reporting to the Joint IG Board is responsible for ensuring that this policy is implemented, that the records management system and processes are developed, co-ordinated and monitored, and that regular audits of practice are undertaken.

9. ABBREVIATIONS / DEFINITION OF TERMS USED

ABBREVIATION	DEFINITION
DPA	Data Protection Act
GDPR	General Data Protection Regulations

TERM USED	DEFINITION
Corporate Record	Corporate records are **non-clinical**, i.e. all administrative records (e.g. personnel, estates, finance etc.).
Information Assets	An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively. Information assets have recognisable and manageable value, risk, content and lifecycles. Corporate records can be defined as Information Assets.

APPENDIX 1 – CORPORATE RECORDS PROCEDURES

a) General Principles

The key components of corporate records procedures are:

- record creation;
- record keeping;
- record maintenance (including tracking of record movements);
- access and disclosure;
- closure and transfer;
- appraisal;
- archiving; and
- disposal.
- Corporate Records Audit

b) Records Creation

Implementing a common format for the creation of records will ensure that those responsible for record retrieval are able to locate records more easily. The following principles should be practised when creating records:

- Record naming is an important process in records management and it is essential that a unified approach is undertaken within all areas of the Trust to aid in the management of records.
- Staff members should refrain from naming folders or files with their own name unless the folder or file contains records that are biographical in nature about that individual, for example, personnel records.
- The re-naming of old documents is optional but new documents must follow the standard naming convention.
- Version Control is the management of multiple revisions to the same document. Version control enables one version of a document to be distinguished from another.
- Where records contain person identifiable data or corporate sensitive information it is a legal requirement that such data is stored securely. All such data should have the correct protective marker applied to identify the level of confidentiality of the record; - **N.B** *as at 1 April 2014 HM Government identified new categories for protective marking classifications which are being considered by the NHS before adoption.*
- Good record keeping should prevent record duplication. Information Asset Owners should ensure team members have not previously created a record prior to initiating a new one.
- Good record keeping requires information to be recorded at the same time an event has occurred or as soon as possible afterwards.
- In accordance with the Trusts' aim to move to become a largely paperless organisation, staff are encouraged to create records in electronic format wherever applicable

c) Records Keeping

- Each operational unit (e.g Estates, Finance, Complaints, etc) are responsible for generating Corporate Records should maintain a register of the records they own to enable quick and easy retrieval. Registers must be updated when opening a new record and on appraisal and destruction of a record.

- Primary electronic records must be held within shared drives i.e SharePoint or a shared folder on the S:/drive rather than individuals' drives. This ensures that the primary record is easily accessible even in the document owner's absence.
- Short-lived documents such as telephone messages, notes on pads, post-its, e-mail messages, etc. do not need to be kept as records. Unless they are part of a decision making process i.e. if they are business critical, in which case they should be transferred to a more formal document, which should be saved as a record.
- Staff should not use home email accounts or private computers to hold or store any sensitive records or information which relates to the business activities of the Trust
- Records should not be permanently stored on removable media (e.g memory sticks). Removable media must be Trust owned and encrypted. Records should be removed from a memory stick to secure storage as soon as possible. Person sensitive data should not be stored on any removable media

d) Scanning

- For reasons such as business efficiency and/or to address problems with storage space, staff should consider the option of scanning paper records into electronic format. Ricoh Copiers provide a scanning function which will return the document to the User via email.
- Staff members involved in a process to scan paper records into electronic format with the purpose of discarding the original paper file, should understand the principles of information management encapsulated in Code of Practice BIP0008 to conform to the provisions of the Records Management Code of Practice and/or seek advice from the Company Secretary
- A check should be made to confirm that the scanned document, if needed, can be reproduced. If this assurance is made then the original paper file can be destroyed

e) Record Maintenance

- The movement and location of records should be controlled to ensure that:
  - a record can be easily retrieved at any time,
  - any outstanding issues can be dealt with,
    and
  - there is an auditable trail of record transactions.
- A tracking process should be in place to ensure that the whereabouts of records is always known.
- Information Asset Owners should ensure they have a business continuity plan to provide protection for records which are vital to the continued functioning of the organisation
- Records held in electronic format and saved on shared drives, S:drive or SharePoint have regular back-up copies scheduled and undertaken on a daily basis

f) Access and DIsclosure

- There are a range of statutory provisions that give individuals the right of access to information created or held by the Trust, such as a data subject access request, Freedom of Information request and correspondence on how a decision was made.

The Data Protection Act 2018 allows individuals to find out what personal data is held about them. The Freedom of Information Act 2000 gives the public the right of access to information held by public authorities

- Only certain staff members have the authority, which is dictated by their role, to disclose records to external sources The Information Rights Team can be located within the Information Governance Dept. for advice
- It is the responsibility of the IAO to protect access to the records they own within the Trust. Such safeguards include filing in lockable cabinets, password protecting electronic documents, controlling access to shared network drives. IAOs should remove access to files and folders when staff leave the organisation or transfer to another department
- Paper file storage must be safe from unauthorised access and meet fire regulations.

g) Closure and Transfer

- Should there be a requirement to transfer information from one organisation to another the mechanisms for transfer should be tailored to meet the sensitivity of the material contained within the record. Secure bags and if required courier transport should be employed to ensure safe transfer
- As soon as a record has ceased to be active it should be closed (ie. made inactive) and transferred to secondary storage
- It is the responsibility of IAOs to ensure that they have access, if needed, to secondary storage and understand the processes and procedures for using the storage facility. Currently the Trust has a contract with Fastness.

h) Appraisal

- Appraisal refers to the process of determining whether records are worthy of permanent archival preservation, as certain records may be of historical interest
- The purpose of the appraisal process is to ensure the records are examined at the appropriate time to determine whether or not they are worthy of archival preservation, whether they need to be retained for a longer period as they are still in use, or whether they should be destroyed.
- The process to appraise a record begins with validating the timeframe against the retention period to calculate if the record is suitable for destruction A record of the appraisal and the outcome of the decision should be made on the asset register.

i) Archive and Retention

- Corporate Records should be retained in accordance with the Trusts Records Retention Schedule and the Records Management: NHS Code of Practice©.
- The recommended retention periods shown on the Records Retention Schedule (see Appendix 2) apply to the official or master copy of the records. Any duplicates or local copies made for working purposes should be kept for as short a period of time as possible.
- Duplication should be avoided unless absolutely necessary. It should be clear who is responsible for retaining the master version of a record and copies should be clearly marked as such to avoid confusion

- **Unnecessary retention may also incur liabilities in respect of the Freedom of Information Act 2000 and the Data Protection Act 2018**. If the Trust continues to hold information which it does not need to keep, it would be liable to disclose it upon request. The Data Protection Act 2018 also advises that personal data should not be retained longer than is necessary.(storage limitation)

- Recommended minimum retention periods are calculated from the end of the calendar year which corresponds to the start of the record creation.
- Corporate records in paper format are archived in the long term storage facility currently at Fastness. IAOs are responsible for ensuring records are archived.

j) Disposal

- Disposal is the term used to cover the final action taken on records. This will either be destruction or transfer to archival storage.
- When a record has no more value to the Trust or has met its assigned retention period it may be disposed of and destroyed under confidential destruction conditions. All departments must have access to confidential waste bins (ShredIT).
- Not all records will be destroyed once the retention period has been met. Any records that have historical value to the Trust will be sent to the County Archives Centre, where they will be kept for the future of the organisation and may never be destroyed.
- It can be a personal criminal offence to destroy requested information under either the Data Protection Act or the Freedom of Information Act (Section 77). Therefore, the Trust needs to be able to demonstrate clearly that records destruction has taken place in accordance with proper retention procedures. If in doubt about destroying a record, staff members should seek specialist advice from the Company Secretary

k) Corporate Records Audit – Annual Requirement

- To ensure that record management standards are adhered to an annual audit of Corporate Records will be undertaken.
- The audit will ensure that systems and processes are in place for records to be associated with the decision making processes in the Trust.
- The results of the audit will be presented to the Information Governance Board and used to inform a year on year improvement programme

APPENDIX 2 – RECORDS CREATION GUIDANCE – FILING AND NAMING GUIDANCE

What is Records Management?

Records management is the systematic management of records, whatever the media including paper and electronic,

Filing Structures

Appropriate filing and storage of records is essential to ensure their authenticity and reliability and it enables the Trust to obtain the maximum benefit from quick and easy retrieval of information.

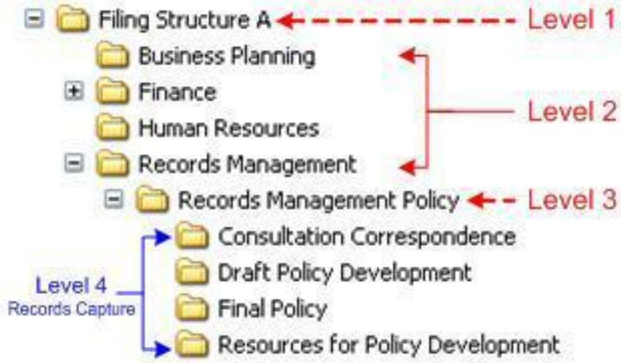
All records should be stored on the S:/drive or on SharePoint never on a Y:/drive (unless it is working copy) and never, under any circumstances, on a the desktop of a PC

Each operational unit in the Trust will adopt a filing system which

- Provides a classification scheme to group or link related records
- Reflects the work of the unit
- Protects records from unauthorised alteration
- Ensures that records are protected from unauthorised access

A filing structure should contain four levels

Level 1 = the function of the organisation e.g. for CPFT this would be the Department – IG, HR, Finance
Level 2 = the activities e.g. the teams with in the dept. or the areas of work e.g. projects, policies
Level 3 = the transactions e.g. shows individual pieces of work or categories in a project
No records are stored in these levels.
Level 4 - Record storage takes place in level 4

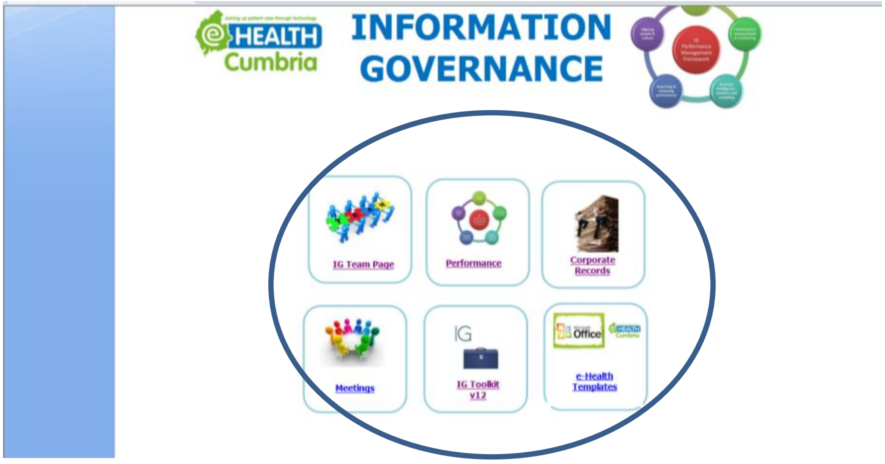


The above is a typical records structure in the S:/ Drive.

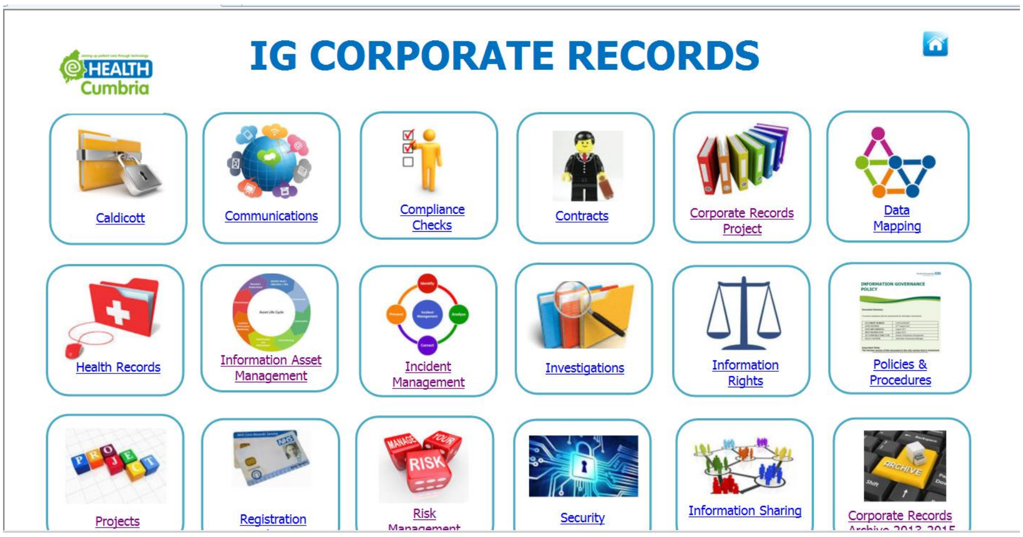
For Sharepoint users the principles are the same although the view may be slightly different:

e.g **Level One** = Information Governance

Level Two:



Level Three



Level 4 - Documents are then stored in the folders beneath these tiles

In SharePoint it is good practice to have a consistent naming convention for documents of the same group, this allows for easy searching. For example all documents relating to a system implementation could begin with SystemName and then the name is completed with whatever the document is about.

How Do I name a record?

Naming conventions are standard rules to be used for naming both documents and electronic folders and are used to make it easier to find records. The Trust follows guidance issued by the National Archives, i.e.

- Give a unique name to each record;
- Give a meaningful name which closely reflects the record contents;
- Express elements of the name in a structured and predictable order;
- Locate the most specific information at the beginning of the name and the most general at the end; and
- Give a similarly structured and worded name to records which are linked (for example, an earlier and a later version).
- Agendas, minutes and meeting papers should be stored in chronological order
- A record should be given a name that will make sense to other people, and that will facilitate locating the record once it is no longer in use.
- Never use your own name, or terms such as ‘Miscellaneous’ as file or document names.
- The title should contain keywords relating to the subject of the record. Keywords should be chosen and structured in such a way as to make searching and retrieval of files an easy and straightforward operation.
- The use of non-specific or generic terms i.e. “general correspondence” should be avoided.
- A date reference may also be used to enable documents with the same titles but different dates to be distinguished.
- The file extension is normally allocated by the application i.e. ‘doc’ or ‘xls’. In general, if you cannot see a file extension, there is no need to add one as it will be assigned automatically by the application you are using.
- All file names must exclude illegal characters. These include \ / *? “ ‘ < > . :
- Anyone creating a document should use the Trust templates which can be found on the intranet.

The Rules

Rule	Explanation	example
Keep file names short but meaningful	Long file names mean long file paths which increase the likelihood of error, are more difficult to remember and recognise. Avoid using initials, abbreviations and codes that are not commonly understood.	✓ Sausageandmashcommittee.doc X The_sausage_and_mash_committee_remit.doc
Repetition/redundant words Avoid duplicating words in the file name which are already used in the folder name	Avoiding duplication leads to shorter file names	Complaints x Complaint from Mr B Brown.doc ✓ BrownBarry20141004.doc

Use capital letters to delimit words, not spaces or underscores	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.	✓ RiskManagement.doc X Risk_management.doc
Numbers Always use two digits in a file name unless it is a date	If only one digit is used the records are ordered out of sequence	x Office procedures 1.doc x office procedures 13. doc x Office procedures 2 .doc ✓officeprocedures01.doc ✓officeprocedures02.doc ✓officeprocedures03.doc
Dates Always use dates 'back to front' so that the year begins the sequence. Avoid using the month names – use numbers instead YYYYMMDD	The chronological order of the records is maintained	Budget sheets x December 2013 x May 2014 ✓ 201312 ✓ 201405
Personal Names When including a personal name in a file name give the family name first followed by the initials	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	✓ BrownSR20041201.doc X SamRBrown20041201.doc
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.	✓AdvertisingV01Draft.rtf ✓BudgetReport2003-2004V15Draft.rtf XDraftAdvertising.rtf X DraftBudgetReport2003-2004.rtf
The most specific information should be at the beginning of the name and the most general at the end	Enables easier searching and retrieval	X MinutesBoard20151005.doc X Board meeting minutes 20151005.doc ✓Boardminutes2015105.doc

Records which are linked (for example, an earlier and a later version) should have a similarly structured and worded name		X Draft strategy report.doc X Final strategy report.doc ✓Strategyreportdraft201511.doc ✓Strategyreportfinal201512.doc
Version numbers 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.	✓ OrgHier2002V02.xls ✓ OrgHier2002V03.xls ✓ OrgHier2002V04.xl X Org_Hier_2002_v2.xls X Org_Hier_2002_v3.xls X Org_Hier_2002_v4.xls

Version Control

What is Version Control?

Version control applies when documents which are likely to be revised and redrafted, such as policies, procedures or regulations, and when you might need to keep a record of how the document changed over time.

The recommended version control system simply gives a number to each version of a document. For example:

Version	Document Name
Initial draft	Strategic Plan Version 0.1.doc
2nd draft	Strategic Plan Version 0.2.doc
3rd draft	Strategic Plan Version 0.3.doc

A Version Control Table may be inserted at the beginning of the document. This approach may be necessary for documents where there are legal or regulatory reasons for having a clear audit trail of changes. It is also good practice for all policy documents. For example:

Version	Date	Author Changes
0.1	10/02/13	Produced by A. Jones
0.2	11/02/13	A. Jones comments of working group added
0.3	15/02/13	F. Brown amended to include change in procedure section 2.1
1.0	20/02/13	B. Smith Final draft approved by Records Committee

Whichever type of system is adopted, it is important to follow some good practice rules to ensure it works effectively:

Use version numbers of the form 1.01, 1.02, 2.01, etc, where the number before the point indicates the original or a substantively different version and the number after the point, a minor variation on the previous iteration.

Remember that each time a document is redrafted it should be copied and renamed with the appropriate version number.

The version numbers and date must be on the document cover and in the footer text of each page.

Include the document name and file path as 'document footer' on each page of the document.

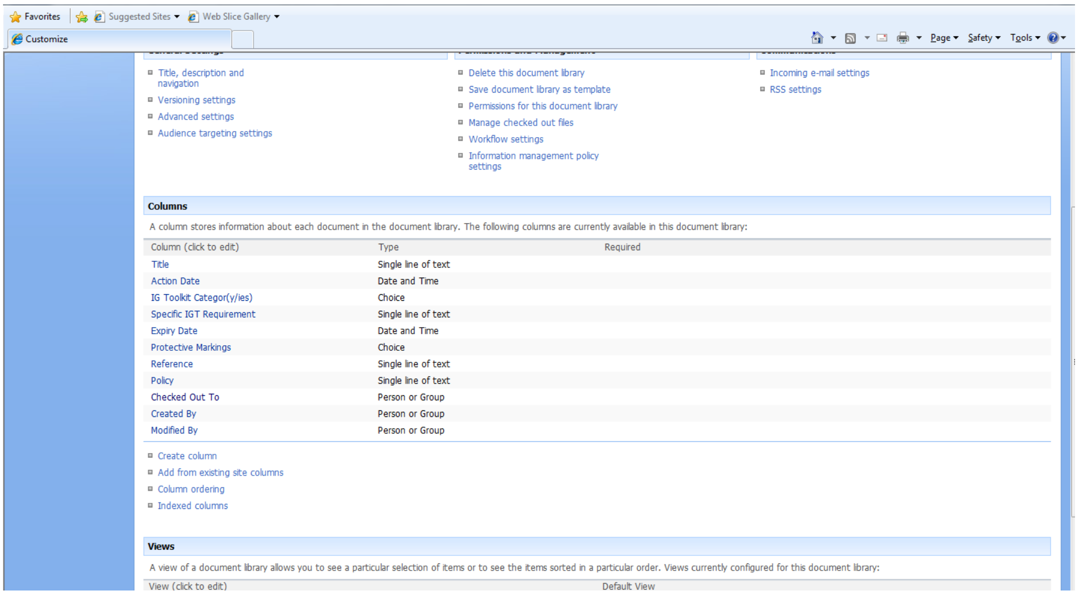
Once the document has been finalised, it should be set as 'read-only' so that it cannot easily be altered.

Headers and Footers

Every document should have footer. It should contain the version number, the date the file name and a page number.

Tracking and Tracing

Records stored in a SharePoint library can be readily tracked by selecting the appropriate columns as the site is created



- Title, description and navigation
- Versioning settings
- Advanced settings
- Audience targeting settings

- Delete this document library
- Save document library as template
- Permissions for this document library
- Manage checked out files
- Workflow settings
- Information management policy settings

- Incoming e-mail settings
- RSS settings

Columns

A column stores information about each document in the document library. The following columns are currently available in this document library:

Column (click to edit)	Type	Required
Title	Single line of text	
Action Date	Date and Time	
IG Toolkit Categor(y/ies)	Choice	
Specific IGT Requirement	Single line of text	
Expiry Date	Date and Time	
Protective Markings	Choice	
Reference	Single line of text	
Policy	Single line of text	
Checked Out To	Person or Group	
Created By	Person or Group	
Modified By	Person or Group	

- Create column
- Add from existing site columns
- Column ordering
- Indexed columns

Views

A view of a document library allows you to see a particular selection of items or to see the items sorted in a particular order. Views currently configured for this document library:

View (click to edit)	Default View

Any departments still maintaining paper records should adopt a tracer card system to record what records have been removed, when they were removed and who by. Records should be returned immediately after use to the original filing system

A Corporate Records Register must be maintained to identify details of records held in a department. The local register should be sent to the Information Governance Dept on an annual basis so that the Trusts central Register can be verified.

Maintenance of the register should be the responsibility of the Information Asset Administrator

Retention, Appraisal and Disposal

IAOs and IAAs should refer to the Corporate Records Retention Schedule which provides information on the types of records held in the Trust, their retention period and disposal method

DOCUMENT CONTROL

Equality Impact Assessment Date	N/A
Sub-Committee & Approval Date	Joint Corporate Records Group 09/08/2018

History of previous published versions of this document:

Trust	Version	Ratified Date	Review Date	Date Published	Disposal Date
NCUH	3.0	24/10/2013	31/10/2015	28/10/2013	31/10/2023
CPFT	N/A	20/04/2015	30/04/2018	20/04/2015	30/04/2025

Statement of changes made from previous version

Version	Date	Section & Description of change
0.1	26 July 2018	• Head of Information Governance – versions for both trusts reviewed and brought together as an aligned policy for the first time. Therefore considered as a replacement policy for each Trust.

List of Stakeholders who have reviewed the document

Name	Job Title	Date
Corporate Records Group	As per membership	11/08/2018