



London Ambulance Service **NHS**
NHS Trust

Records Management and Information Lifecycle Policy

DOCUMENT PROFILE and CONTROL.

Purpose of the document: To define a structure for the LAS to ensure adequate records are maintained and they are managed and controlled effectively and at best value, commensurate with legal, operational and information needs for the duration of their lifecycle.

Sponsor Department: Information Governance

Author/Reviewer: IG Manager. To be reviewed by March 2021.

Document Status: Final

Amendment History			
Date	*Version	Author/Contributor	Amendment Details
15/05/18	3.7	IG Manager	Further minor changes relating to new Data Protection legislation
10/03/18	3.6	IG Manager	Review and minor revisions
05/05/16	3.5	IG Manager	Enhanced S.11
25/03/15	3.4	IG Manager	Document Profile and Control update
16/12/14	3.3	IG Manager	Review and minor amendments
23/09/11	3.2	IG Manager	S.10 amended by IGG.
21/09/11	3.1	IG Manager	Addition to S.10 plus change to S.11 requested by ADG.
25/02/2011	2.1	Head of RM	Minor amendments and Appendix1 added.
07/07/2010	1.3	Director of Corporate Services/ Director of IM&T	Amendments
17/06/2010	1.2	Head of Records Management & BC	
01/10/2009	1.1	Head of Records Management & BC	
01/12/2005	1.0	Head of Records Management	First issue

***Version Control Note:** All documents in development are indicated by minor versions i.e. 0.1; 0.2 etc. The first version of a document to be approved for release is given major version 1.0. Upon review the first version of a revised document is given the designation 1.1, the second 1.2 etc. until the revised version is approved, whereupon it becomes version 2.0. The system continues in numerical order each time a document is reviewed and approved.

For Approval By:	Date Approved	Version
IGG	13/03/18	3.6
IGG	06/01/15	3.3
IGG	27/05/11	3.0
SMG	14/07/2010	2.0
Ratified by:		
ADG	24/08/11	3.0

Published on:	Date	By	Dept
The Pulse (v3.7)	25/05/18	Internal Comms team	Comms
The Pulse (v3.5)	06/05/16	Governance Administrator	G&A
The Pulse	26/03/15	Governance Administrator	G&A
The Pulse	19/10/11	Governance Administrator	GCT
LAS Website (v3.7)	25/05/18	Internal Comms team	Comms
LAS Website (v3.5)	06/05/16	Governance Administrator	G&A
LAS Website	26/03/15	Governance Administrator	G&A
LAS Website	19/10/11	Governance Administrator	GCT
Announced on:	Date	By	Dept
The RIB	08/2010	Records Manager	GCT

EqIA completed on	By
12/08/10	Head MI; Head Legal; Head PED; Head RM
Staffside reviewed on	By

Links to Related documents or references providing additional information		
Ref. No.	Title	Version
	Public Records Acts 1958 and 1967	
	Data Protection Act 2018	
	Freedom of Information Act 2000	
	Records Management NHS Code of Practice	
	Caldicott Review of Patient Identifiable information, 1997, Caldicott 2 and 3 Reports	
	Audit Commission, Setting the Record Straight, 1995.	
TP/017	Procedure for the Management of Health Records	
TP/009	Policy for access to Health Records	
TP/047	Electronic Information Handling Procedure	
TP/057	Waste Management Policy	
TP/030	Retention and Disposal Policy and Procedure	
TP/024	Procedure for Managing Patient Confidentiality when Dealing with the Media	
	NHS Information Governance: guidance on legal and professional obligations (DH 2007)	

Document Status: This is a controlled record as are the document(s) to which it relates. Whilst all or any part of it may be printed, the electronic version maintained in P&P-File remains the controlled master copy. Any printed copies are not controlled nor substantive.

Ref. TP/029	Title: Records Management & Information Lifecycle Policy	Page 3 of 17
--------------------	---	---------------------

1. Introduction

The London Ambulance Service NHS Trust (LAS) is dependent on its records to operate efficiently and account for its actions. This policy defines a structure for the LAS to ensure adequate records are maintained and they are managed and controlled effectively throughout their lifecycle and at best value, commensurate with legal, operational and information needs.

Our organisation's records are our corporate memory, providing evidence of actions and decisions and representing a vital asset to support our daily functions and operations. They support policy formation and managerial decision-making, protect the interests of the LAS and the rights of patients, staff and members of the public who have dealings with the LAS. They support consistency, continuity and efficiency and productivity and help us deliver our services in consistent and equitable ways.

Records management, through the proper control of the content, storage and volume of records, reduces vulnerability to legal challenge or financial loss and promotes best value in terms of human and space resources through greater coordination of information and storage systems.

The key components of records management are:

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

2. Scope

This policy covers all records held by the Trust relating to information, created or received in the course of business, and captured in a readable form in any medium, electronic or otherwise, providing evidence of the functions, activities and transactions of the organisation. They include:

- Health records
- Personal data as defined by Data Protection legislation.

- Corporate and administrative records (including personnel, estates, financial and accounting records, contract records, litigation and records associated with complaint-handling)
- Electronic mail
- Photographs, slides, and other images
- Microform (i.e. fiche/film)
- Audio and video material

They do not include copies of documents created by other organisations such as the Department of Health, kept for reference and information only.

All records created in the course of the business of the trust are corporate records and are public records under the terms of the Public Records Acts 1958 and 1967. This includes email messages and other electronic records.

3. Objectives

1. To provide a framework for the systematic management of all health and corporate records created and used by the LAS throughout their lifecycle.
2. To provide assurance that records will be accessible but secure and produced to an acceptable quality.
3. To encourage awareness of the importance of records management and the need for responsibility and accountability at all levels.
4. To be in compliance with legal and statutory requirements.
5. To achieve efficiency and best value through improvements in the quality and flow of information.
6. Through effective information management to reduce the risks associated with the handling of sensitive records such as health and personal material and documents that are protectively marked.

4. Responsibilities

The **Chief Executive** has overall responsibility for ensuring that records are managed responsibly within the Trust.

The **Chief Information Officer** is the Senior Information Risk Owner (SIRO)

Ref. TP/029	Title: Records Management & Information Lifecycle Policy	Page 5 of 17
-------------	--	--------------

The **Director of Corporate Governance** has strategic responsibility for Information Governance including records management throughout the Trust.

The **Caldicott Guardian** is responsible for protecting the confidentiality of patient and service-user information and this policy supports the Caldicott function.

The **Information Governance Manager** is responsible for the management of records in the organisation and identifying key corporate records and providing guidance and advice on their management and retention.

The **Information Governance Group (IGG)** will monitor the implementation of this policy.

The **Executive Leadership Team**, and **Heads of departments** are responsible for ensuring that the policy is implemented in their directorates and individual departments. They will nominate **Information Asset Owners**, who will liaise with the Information Governance Manager on the management of records in each directorate.

Records management responsibilities will be written into all accountable individuals' job descriptions and clear procedures for retention of key records issued. It is the responsibility of **all staff** to ensure that they keep appropriate records of their work in the Trust and manage those records in keeping with this policy and with any guidance subsequently produced by the Information Governance Manager.

5. Definitions

Record – 'Recorded information, in any form, created or received and maintained by the Trust in the transaction of its business or conduct of affairs and kept as evidence of such activity'.

Health Record –

The Data Protection Act 2018 states that a Health Record means a record which:

(a) consists of data concerning health, and

(b) has been made by or on behalf of a health professional in connection with the diagnosis, care or treatment of the individual to whom the data relates;

Information Lifecycle - The life of a record from its creation/ receipt through the period of its 'active' use, then into a period of 'inactive' retention (such as closed files which may still be referred to occasionally) and finally either confidential disposal or archival preservation.

6. Legal and Professional Obligations

Ref. TP/029	Title: Records Management & Information Lifecycle Policy	Page 6 of 17
-------------	--	--------------

All NHS records are Public Records under the Public Records Acts. The Trust will implement all necessary measures to comply with its legal and professional obligations for public records as set out in the Information Governance Alliance 'Records Management: Code of Practice for Health and Social Care', in particular:

- Public Records Acts 1958 and 1967
- Data Protection legislation
- Freedom of Information Act 2000
- The Caldicott Reviews
- Confidentiality: NHS Code of Practice

and any new legislation affecting records management as it arises.

7. Record creation

Records are created to ensure that the business of the Trust is carried out effectively and information is available to:

- support the care process and the continuity of care
- support day to day business which underpins delivery of care
- support sound corporate and managerial decision making and provide evidence of decisions taken
- meet legal requirements, including requests from service users under access to health records legislation
- assist with clinical and other audits and learn lessons from past experience
- support improvements in clinical effectiveness through audit and research

8. Quality of Records

All records must be fit for purpose, complete and accurate and the information they contain reliable with its authenticity guaranteed. Failure to ensure that data is of good quality and is up-to-date could have a detrimental effect on the Trust, its employees, its relationship with other Trusts and the community it serves. The LAS aims to ensure that:

Ref. TP/029	Title: Records Management & Information Lifecycle Policy	Page 7 of 17
--------------------	---	---------------------

- the right information is created at the right time;
- the information is reliable and accurate;
- the information has been created in an appropriate format;
- information has been captured which describes its purpose, its content, who created it, and when it was created (known as metadata).

Except where indicated below all records, such as Corporate Records will be created electronically and or stored electronically. The LAS will aim to manage electronic records to show proof of their validity and authenticity so that any evidence derived from them is clearly credible and authoritative.

Paper records will primarily be health and other manually completed forms and records which are required to be kept in hard copy for legal purposes such as signed contracts. All manually completed paper records must be written clearly and legibly using a black ink ballpoint pen. Records should be dated and signed with time of entry and any alterations should be visible and initialled. When forms are self duplicating, staff must ensure that all written entries are legible on all copies. See TP017 for further details on the completion of such records.

9. Management and Tracking of Records

Accurate recording and knowledge of the whereabouts of all records is essential if the information they contain is to be located quickly and efficiently. Health records are managed and tracked through the application of TP017 Procedure for the Management of Health Records.

The Trust aims to introduce this to achieve a controlled environment for the management and tracking of unstructured records.

10. Storage, Handling, and Security

The storage of paper records will be kept to a minimum and applies primarily to health records which have not been scanned. Health records will be stored securely as detailed in TP017 Procedure for the Management of Health Records.

The location of paper records will be controlled to ensure that a record can be easily retrieved at any time. Storage accommodation for records should be clean and tidy in order to prevent damage to the records. Equipment used for these records should provide storage that is safe from unauthorised access and that meets fire regulations but that allows maximum accessibility to the information commensurate with its frequency of use.

Staff must ensure that all records, in particular patient confidential data (PCD), are kept secure at all times when being handled and/or transported between Trust locations and externally. All portable devices

Ref. TP/029	Title: Records Management & Information Lifecycle Policy	Page 8 of 17
--------------------	---	---------------------

containing electronic records must be encrypted and the transportation of patient confidential paper records, particularly externally, must be kept to a minimum and not stored externally except under controlled conditions. (See also TP047 Electronic Information Handling Procedure).

Records will be kept secure from unauthorised or inadvertent alteration or erasure and will be held in a robust format which remains readable for as long as records are required.

In the majority of cases the record will be electronic and hard copies will only be kept on a temporary basis for local use. Electronic records will be stored in their respective databases or, in the case of unstructured data, on network drives with restricted access where required, especially with regard to PCD. Electronic documents must not be kept on local hard drives as there is a risk that they may be lost, they are not controlled, and this prevents access to others.

11. Disclosure and Retrieval

Records and the information within them will be accessible so they can be efficiently retrieved by those with a legitimate right of access, for as long as the records are held by the organisation.

Health records will only be disclosed by the LAS in compliance with TP009 'Policy for Access to Health Records, Disclosure of Patient information: Protection and Use of Patient Information'. No such personal identifiable information must be disclosed through social media websites and when making contact with the media all staff should follow TP024 'Procedure for Managing Patient Confidentiality When Dealing with the Media'.

Any secondary use of health records will be anonymised wherever this is sufficient for purpose and disclosure of PCD to a third party will be limited to the minimum information required to satisfy the purposes of disclosure. Any bulk or regular transfer of PCD between the LAS and other Trusts and agencies will be controlled and monitored through an Information Sharing Agreement (ISA). The Trust has a template for an ISA and all ISAs are considered for approval by the Information Governance Group before they are signed off by the Trust's Caldicott Guardian or the SIRO. The IG Manager maintains a register of all approved ISAs.

12. Retention, Disposal, and Destruction

The Trust will develop a consistent and documented approach to retention and disposal which will include retention and disposal schedules as set out in the IGA Records Management Code of Practice for Health and Social Care 2016 Section 4.

Ref. TP/029	Title: Records Management & Information Lifecycle Policy	Page 9 of 17
--------------------	---	---------------------

Health records will be retained and disposed of in accordance with TP017 Procedure for the Management of Health Records and the IGA Records Management Code of Practice for Health and Social Care 2016 Section 4.

E-mails must be retained for the same period of time as the categories of record to which they are related and must be disposed of and destroyed in the same way as other electronic documents.

The IAO with responsibility for the records also has the responsibility to ensure that a review is carried out at the end of the retention period. Where there is uncertainty about the need for continuing retention the IAO will consult with the Information Governance Manager who will make the final decision on retention.

The IAO with responsibility for the records is responsible for their secure destruction. Electronic records will be destroyed in compliance with TP047 Electronic Information Handling Procedure and paper copies will be destroyed securely on site in compliance with TP057 Waste Management Policy.

For full details of records inventory and retention please see TP030 Retention and Disposal Policy and Procedure.

13. Implementation

This policy will be implemented through a project to develop and introduce Electronic Document Records Management in the Trust. Pending this the Records Management Good Practice Guidelines apply and these can be found at Appendix1.

IMPLEMENTATION PLAN				
Intended Audience	For all LAS staff			
Dissemination	Available to all staff on the Pulse			
Communications	Revised policy and procedure to be announced in the RIB and a link provided to the document			
Training	Records management training is provided as part of the Governance training for new staff at Corporate Induction and is being introduced in a programme of Information Governance training identified in the LAS Training Needs Analysis for all staff. Specialised training tailored to staff who have responsibility for record-keeping will be developed.			
Monitoring:				
Aspect to be monitored	Frequency of monitoring AND Tool used	Individual/ team responsible for carrying out monitoring AND Committee/ group where results are reported	Committee/ group responsible for monitoring outcomes/ recommendations	How learning will take place
Progress with EDRM implementation	Quarterly Report	IG Manager IGG	Risk Compliance and Assurance Group	Feedback on progress reports

**RECORDS MANAGEMENT
GOOD PRACTICE GUIDELINES**

1. Introduction

To ensure compliance with legislation and standards as well as business efficiency it is necessary for the London Ambulance NHS Trust (LAS) to have systems in place that will enable the information and records created and used by the LAS to be managed effectively so they can be accessed throughout the Trust and located with ease when required.

In order to achieve this in the present environment it is necessary to create a managed network environment and a structured approach to electronic file/folder and document management without the benefit of having an Electronic Document Records Management system in place.

These guidelines have been produced to enable staff to carry out effective records management at the local level. They apply to all records, primarily electronic, but also specifically apply to paper records where indicated. They outline the good practices designed to ensure the efficient management of information across the organisation and should be used by all departments and teams.

2. Administration

Documents must be managed effectively at the local level for information to be located easily. All departments will identify a key member of staff, or more than one where teams break down into smaller units, who will act as Information Asset Owners (IAOs) for the management of their records and information, both electronic and hard copy, to ensure that the good practices outlined below are maintained.

3. Document creation

Documents, when created, must be given meaningful names to reflect their subject content in order to facilitate effective searching, but very long path names should be avoided. They should have the most specific information at the beginning of the name and the most general at the end and names must be similarly worded when documents are linked (e.g. different versions of the same document). Where date order is required the date should be entered before the document title and in YYYY-MM-DD format. Version control should

Ref. TP/029	Title: Records Management & Information Lifecycle Policy	Page 12 of 17
--------------------	---	----------------------

also be used where appropriate and follow major or minor versions (i.e. v1 or v1.1) format. When creating a document authors should also enter information about the document (metadata) such as title, subject, and keywords (in Word & Excel 2007 use the 'Office' button at the top left of the screen and then click on 'Prepare' followed by 'Properties'). Consideration should be given to whether or not the document should be protectively marked and if so it will need to be kept in a secure folder and/or encrypted (See Section 7). Once a document has been created it should be placed in the appropriate network drive being saved into a folder at the lowest level of the department's fileplan. A final document should in effect be declared a record (in Word & Excel 2007 use the 'Office' button at the top left of the screen and then click on 'Prepare' followed by 'Mark as Final') which makes the document 'read only'.

4. Drive areas/folders

Departments must ensure good discipline in the correct maintenance of their drive areas. These should be created in a network drive and organised in a hierarchy, but for ease of searching should not descend by more than 4-6 levels. It is preferable to match the folder structure to the structure of the Inventory/Retention Schedule wherever possible as this will ease the disposal process.

At the top should be the department name followed by the individual functional/subject areas under that department. i.e.:-

Governance and Compliance

- Audit
- Information Governance
- Risk

At the next level IAAs should create folders and sub-folders (where required) that describe activities (or subjects) under each function, then at the lowest level transaction folders that contain documents.

➤ Please avoid:-

- Folders and documents at the same level. Always break subjects down into their component parts and create folders for each part. i.e.:-

```

Information Governance      }
Records Management        }
Corporate Documents        } No documents here
Trust Policies              }
TP012 Data Protection Policy }
Document Revisions        > Documents at this level
  
```

- Naming folders after individuals' names as these can include a host of unrelated documents.
- Folders called 'Archive'. If Electronic folders are to be 'archived' to save space on the network this should be carried out when a folder is 'closed' and the folder name should be maintained. A record of all

Ref. TP/029	Title: Records Management & Information Lifecycle Policy	Page 13 of 17
-------------	--	---------------

'archived' folders should be maintained for all documents that are kept off-line on CD ROM or DVD as they will not be searchable over the network.

- Folders called 'New Folder', 'Working Folder', 'Ad Hoc', or 'General' etc.as these are meaningless terms. You may know what is in them but no-one else will.
- Folders with duplicate or very similar titles in the same part of the fileplan, even at different levels, as this leads to confusion - Keep related subjects together as much as possible.
- Empty folders

To ensure good drive/folder discipline all teams should channel new folder creation through their IAOs so that an overview of the folder structure can be maintained. IAOs will then need to ensure that new documents are not saved in inappropriate folders by making regular checks. Documents should never be stored on hard drives (E-Drive or C-Drive), unless personal to the user, as they will not be backed-up nor accessible to others if required.

5. Paper

All paper should be kept to a minimum and records should be scanned wherever possible. Working documents or reference copies of external publications should be the main paper kept. Where, for the time being, it is still necessary to keep some paper records they should be placed in clearly marked files and a 'plan' or structure should be defined with a referencing system (alphanumeric is best) if the amount of paper files warrants this for ease of retrieval. Where a considerable number of records are still kept in paper and are likely to be moved between departments on a regular basis a basic tracking system will need to be set up (see IG Manager for further details). A spreadsheet (Inventory/Retention Schedule) should be kept of all files and the documents contained within them detailing the review date and reviewer of each file. As storage space is at a premium teams will be expected not to add to their paper storage but to manage it effectively in order that paper copies are kept for as short a time as possible. All departments should scan in general correspondence and as much paper received by the Trust as possible unless it is only to be kept temporarily or it is of a size or type to render this impractical.

6. E-mails

It is the responsibility of all members of staff to manage their email messages appropriately as they can constitute part of the formal record of a transaction. IAOs must ensure that their teams distinguish between emails, both sent and received, that constitute a record of their work and ephemeral email messages. If an email message is to be captured as a record it should be moved from personal mailboxes, located with other records relating to the same business activity on shared drives, and managed in the same way as other records. Emails captured as records are subject to the Inventory/Retention Schedules of the Trust and will be stored and disposed of

Ref. TP/029	Title: Records Management & Information Lifecycle Policy	Page 14 of 17
--------------------	---	----------------------

in the same way as the Trust's other records. Ephemeral email messages should be managed within the mailbox and kept only for as long as required before being deleted.

If public folders are used within teams the IAO must identify one person who can take ownership of the folder or mailbox. This person should be responsible for ensuring that the topics do not change too radically from the purpose for which the folder was created and agreement needs to be determined between the owner of the public folder and the local IAO when to delete email messages (the retention period) and the types of email messages that should be treated as records. Decisions need to be documented.

7. Storage and Security

Live electronic documents should be stored on network drives as covered in sections 3 and 4 and should be protected where appropriate. For example any document containing personal information should be regarded as confidential irrespective of whether it is marked as such, and access to the document must be restricted either by limiting access to the folder or by adding encryption to the actual document (in Word & Excel 2007 use the 'Office' button at the top left of the screen and then click on 'Prepare' followed by Encrypt Document) or both. Electronic documents kept off-line on portable media must be physically protected. Only CD Roms or DVDs (not re-writable) should be used for permanent records and if containing personal or sensitive information they must be encrypted and kept in secure storage. USB keys must be encrypted but should not be used for permanent storage of records and Smartphones and iPADS should be treated in a similar way. Personal and other sensitive information must not be transferred from LAS hardware to personal PCs or portable media such as laptops, iPADS, USB keys, mobile phones, CD Roms etc. unless both permission has been given by the line manager and the documents in question are encrypted or password protected.

Paper storage should be kept to a minimum and if containing personal or sensitive information must be stored securely in locations where they can be easily retrieved if access is likely to be required on a regular basis. Paper health records should be stored securely as detailed in TP017 Procedure for the Management of Health Records. If archived paper has not been scanned it may be placed into 'deep storage' off site if access will only occasionally be required. Secure off - site storage can be arranged for other archived paper if required but costs will need to be met by the department/Directorate concerned. IAOs need to ensure that they keep a spreadsheet (Inventory/Retention Schedule) that details all paper (and off-line electronic) records kept, whether in 'live' files or in an archive.

8. Review/Disposal

IAOs have the responsibility to ensure that records are reviewed and/or disposed of at the correct time as indicated by their Inventory/ Retention

Ref. TP/029	Title: Records Management & Information Lifecycle Policy	Page 15 of 17
--------------------	---	----------------------

Schedule. (See TP030 Records Management Retention and Disposal Policy and Procedure for further detail).

9. Archiving

Archiving of paper records should be kept to a minimum but carried out as necessary using the agreed procedures as detailed in TP030 Records Management Retention and Disposal Policy and Procedure. Also see TP030 for electronic archiving and sections 4 and 7 of this document.

Appendix 1: Duties of Information Asset Owners (could be delegated to an Information Asset Administrator)

For each team the designated IAO will:-




1. Ensure the correct naming of documents saved to folders and the correct naming of folders.
2. Ensure that the team has an appropriate and logical fileplan that is fully utilised and based on function/subject/activity wherever possible.
3. Supervise the creation of new folders for the team.
4. Manage team folders within the drive ensuring that documents are saved to the correct folders and only to the lowest level folder.
5. Ensure that 'loose' documents are assigned to the correct folders.
6. Ensure that paper records are minimised but that any identified are maintained in clearly marked files (folders), based on the structure of the electronic fileplan if possible, and details of the files are kept.
7. Ensure that paper records are scanned into the system wherever possible, removing duplicate paper documents wherever possible.
8. Maintain the Retention/Disposal Schedule recommending changes where records/information categories, retention requirements, or reviewer posts change.
9. Ensure that records/documents are reviewed at the correct time as indicated by the Retention/Disposal Schedule, maintaining a record of review/disposal decisions and actions.
10. Archive appropriate paper records ensuring that a listing is kept of all boxes which details the documents/records contained, the date archived and the review/disposal date with the identified reviewer (see template).

Ref. TP/029	Title: Records Management & Information Lifecycle Policy	Page 16 of 17
-------------	--	---------------

11. Liaise with the Information Governance Manager as required in order to develop and review effective records management practices.

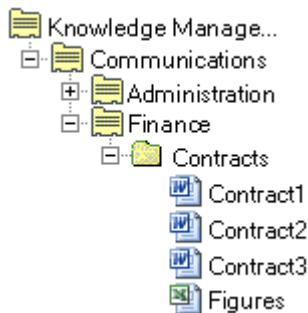
Appendix 2: Electronic File Structure

Similar to Windows Explorer, the electronic structure or fileplan can have many levels of folders, subfolders and documents (files). However, to manage records effectively different rules, and even different names, apply to the different levels:

Name	Rules
 'Class' – the top level. High level grouping such as 'Knowledge management and communications directorate'	A class can only hold sub-classes
 'Sub-class' - Any subsequent level (apart from the final level), e.g. 'External relations team' or 'Finance'	Sub-classes can hold other sub-classes or folders, but not both, and cannot hold documents
 'Folder' - Final level. This is where all documents are stored and grouped together.	Folders can only hold documents

So: a class can hold sub-classes; a sub-class can hold other sub-classes OR folders, but not both. Documents can only be stored at the folder level.

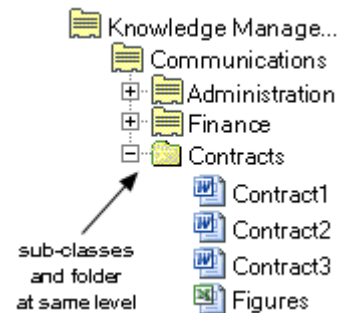
This is correct:



...but this isn't:



...and nor is this:



This structure is designed to ensure that there are no 'loose' documents (documents that are stored in an 'ad-hoc' way with little thought to their indexing or management) so that all can be easily located.

Ref. TP/029	Title: Records Management & Information Lifecycle Policy	Page 17 of 17
-------------	--	---------------