Service
Policy
Instruction

HEREFORD & WORCESTER HWFR FIRE AND RESCUE SERVICE

Records Management

Folder Name	Management & Administration	Folder Number	4
Section Name	Information Management	Section Number	L
Part Name	Records Management	Part Number	5

Status	LIVE
Document Version	Version 02.02
Author	Information Governance Officer
SLB Sponsor	Nigel Snape
Directorate	Legal Services
Date Approved	23/05/2023
Review frequency	2 Years
Next Review	23/05/2025

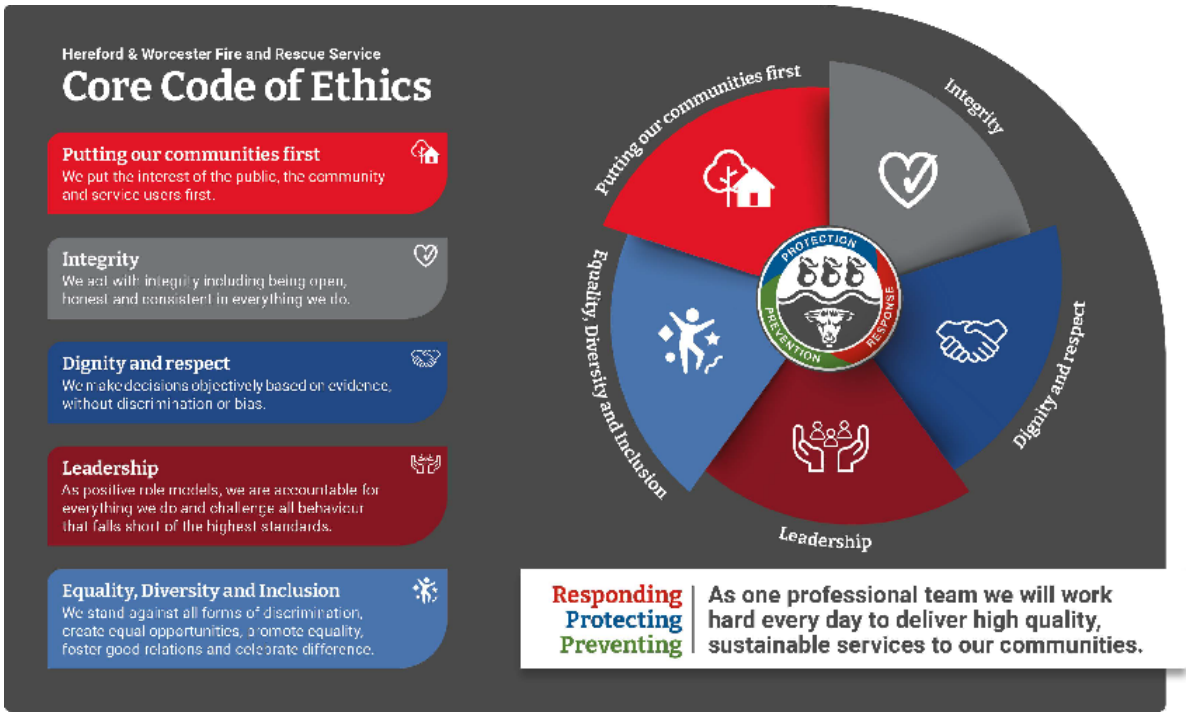
Version History		
Version	Date	Description
1.00	28/02/2017	Published
2.00	21/02/2018	Revised and Published
2.01	21/02/2020	Reviewed – No Changes
2.02	23/05/2023	Revised and Published

Executive Summary

This policy sets out Hereford & Worcester Fire and Rescue Service's (HWFRS) Records Management Procedure to ensure that documents in electronic or physical form are managed correctly and systems are controlled and processes are in place to ensure the protection of Information Systems and data.

Core Code of Ethics

The Core Code of Ethics for Fire and Rescue Services in England sets out five ethical principles, which provide a basis for promoting good behaviour. The Service is committed to the ethical principles of the Code and used them as guidance when forming Service's values. The principles of the Code are reflected in this policy as well.



Alternative Formats

If you require this document in another format please contact the Human Resources and Development Department.

Contents

Records Management

1. Introduction

1.1 All Hereford & Worcester Fire and Rescue Service (HWFRS) employees must ensure they are familiar with the contents of this policy, which describes the standards of practice required for the management of Service records. It is based on current legal requirements and professional best practice.

1.2 All organisations need to keep records and the general public rightly expect that the Service maintains records on its activities and decisions that affect their safety and that of the organisation.

1.3 This guidance describes best practice principles and standards that must be used by HWFRS personnel to:

- Improve the quality and reliability of files and records
- Be clear about what information is stored, how it is stored and where it is stored
- Meet a number of statutory requirements to hold information securely, accurately and reliably; for example, the Freedom of Information Act 2000 (FOIA) and data protection requirements (Data Protection Act 2018 / UK General Data Protection Regulations).
- Comply with the requirements of the Service's Information Security Framework
- Follow the International British Standard for Records Management principles (ISO 15489:2016)

1.4 Records and Documents are different. Documents consist of information or data that can be structured or unstructured and accessed by employees. Records provide evidence of the activities of the Service's functions and policies. Records have strict compliance requirements regarding their retention, access and destruction, and generally have to be kept unchanged (forensically untouched). Conversely, all records are documents.

1.5 This guidance applies to:

- All information in electronic format, including email, paper, digital, social media, videos and telephone messages.
- All documents which exist only in paper format
- Original signed documents
- Master copies of Service documents

2. Background

2.1 HWFRS documents, electronic records or physical paper files, need to be handled in a way which takes into account any associated risks to ensure they are accurate, up-to-date, appropriately available and approved by authorised individuals.

2.2 Authoritative documents are those that are vital to successful service delivery, which could substantially reduce the ability of the Service to meet business requirements or to protect safety, health, environment or property if compromised. These include, for example, pre ratified Fire Authority reports, Business Continuity arrangement and key Service Policy / Instructions (SPIs).

2.3 HWFRS must comply with legal records management requirements. These include but are not limited to the:

- Public Records Act (PRA) 1958 - Formed the main legislation governing public records and established a consistent framework for public records management.
- Local Government Act (LGA) 1972 - The Act reformed local government in England and Wales and provide instruction on the management of local authority's administrative records.
- Data Protection Act 2018 - Is the main piece of legislation that governs the protection of personal data within the UK and defines how data relating to identifiable living people must be processed. The DPA is supported by the UK General Data Protection regulation.
- Freedom of Information Act (FOIA) 2000 - The Act provides a "right of access" to information held by public authorities, either through proactive publication of information or through responding to specific information requests.
- Environmental Information Regulations (EIR) 2004 – The Freedom of Information Act provides access to most other types of information held by public authorities; however information relating specifically to environmental information is covered by the 2004 Regulations.

2.4 In addition to the above, there are legal and professional obligations that affect the management, use and disclosure of information. Guidance is available in the Information Security Policy Framework.

2.5 Failure to comply could result in impairment of service delivery or reputational damage. If there is a significant breach of personal data, a financial penalty of up to £500,000 may be imposed under DPA by the Information Commissioner. With the introduction of GDPR, this fine is increased to up to €10 million or 2% of the Service's annual turnover (whichever is the greater). Failure to comply with relevant Service Information Management policies and the Information Security Policy Framework will be viewed as a serious matter and disciplinary action may be taken where appropriate.

3. Roles and Responsibilities

3.1 The Head of Legal Services supported by the Information Governance Officer has lead responsibility for Information Governance within the Service and for ensuring that a culture which values and protects information assets is fostered.

3.2 The Assistant Chief Fire Officer as the Senior Information Risk Owner (SIRO) is responsible for Records Management at Senior Leadership Board (SLB) level and is in charge of developing and adopting relevant policies.

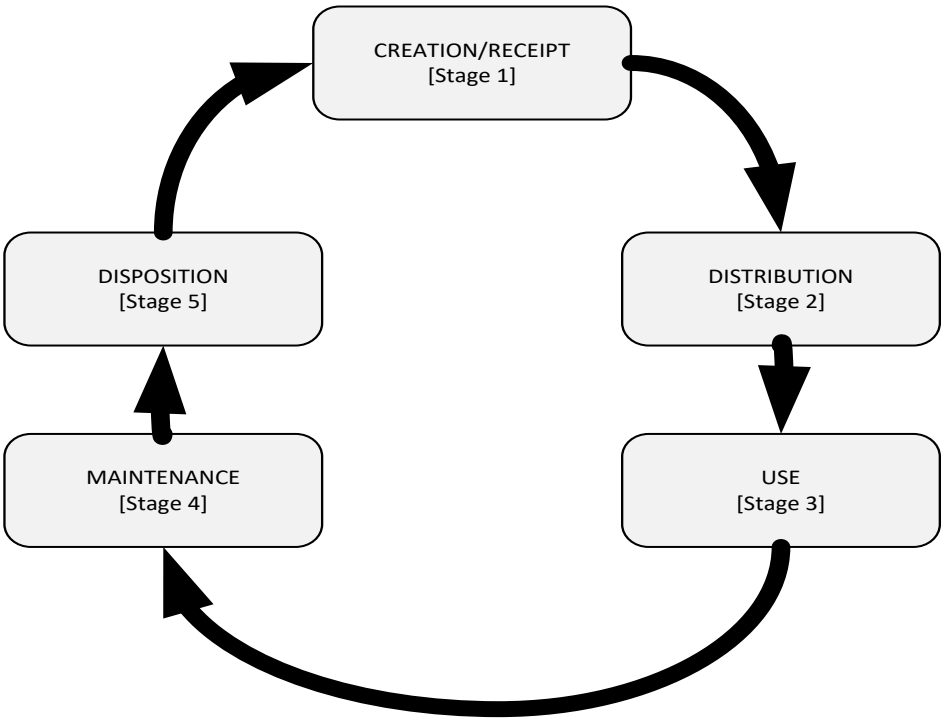
3.3 The Information Governance Officer (IGO) is responsible for the overall development and maintenance of the Records Management Framework and ensuring compliance with legal and regulatory requirements. The IGA is also responsible for monitoring compliance with this policy and assessing its overall effectiveness.

3.4 Department Heads / Group Commanders, as Information Asset Owners (IAO) are responsible for guaranteeing records are processed and managed in accordance with the Overarching Information Governance Policy. They are also responsible for completing and maintaining the Information Asset & Retention Register and ensuring their staff adhere to any relevant procedures and complete any information governance training.

4. Records and Information Life Cycle Management

4.1 Records and Information Management plays an integral role within the Service as it underpins effective information sharing within the organisation and externally to other partner organisations and suppliers.

4.2 The law requires certain records to be kept for a defined retention period, however, records are used on a daily basis for internal purposes to help make decisions, provide evidence, etc. There are 5 steps in the Records Life Cycle:



Stage 1: Creation and Receipt

The **first phase** of the life cycle is when you start handwriting a document, make an entry into a database or start new electronic document. It can be created by Service personnel or received from an external source.

Stage 2: Distribution

Distribution is managing the information once it is created or received whether it is internal or external. It occurs when records are sent to the correct recipient or are copied. Records are distributed when photocopied; printed, attached to an email, hand delivered or posted etc.

Stage 3: Use

This stage takes place after information is distributed. This is when records are used on a day to day basis to help generate organisational decisions, document further action or support other Service related operations. It is also considered the **Active Phase**.

Stage 4: Maintenance

Maintenance is when records are not used on a day to day basis and are stored in a relevant filing system. Even though they are not used daily, they will be kept for legal or financial reasons until they have met their retention period. The maintenance phase includes filing, transfers and retrievals. The information may be retrieved during this period to be used as a resource for reference or to aid in a business decision. Original records should not be removed from the filing system; instead the information should be copied and tracked to ensure no unauthorised amendments were made.

Stage 5: Disposition

Disposition is when a record is less frequently accessed, has no more value to the Service or has met its assigned retention period. It is then reviewed and if necessary destroyed under confidential destruction conditions. Not all records will be destroyed once the retention period has been met. Any record that is still considered to have value for the Service will be kept and archived. This is the final phase of a records lifecycle.

5. Records Retention

5.1 Keeping unnecessary records wastes staff time, takes up valuable space and can incur unnecessary costs; for example where additional servers or extra physical archive storage space has to be purchased. It also imposes a risk liability when actioning requests for Service information or personal data.

5.2 Records should only be destroyed as per the Information Disposal Policy . It is an offence to destroy information under either DPA, GDPR or FOIA once it has been requested by an individual or before the retention period has expired. Therefore, the Service needs to be able to demonstrate clearly that records destruction has taken place in accordance with proper retention procedures.

6. Information Asset and Retention Register

6.1 Categories of Service information are recorded on the Information Asset and Retention Register (IARR).

6.2 The IARR details what the asset is, the owner, where it is located, retention periods and disposition methods.

6.3 GDPR requires considerably more detail about each information asset, to ensure data ownership, accountability and information lifecycles. Additional requirements include but are not limited to, Data Controller and Processor details, access controls, sharing arrangements and Risk ratings.

6.4 Any changes to the way an information asset is managed (processed) must be recorded on the IARR

6.5 Further information on Records Management and Disposal is available in the Overarching Information Governance Policy.

7. Legal Holds

7.1 A legal hold, also known as a litigation hold, document hold, hold order or preservation order is an instruction directing employees to preserve (and refrain from destroying or modifying) certain records and information (both paper and electronic) that may be relevant to the subject matter of a pending or anticipated lawsuit or investigation. Organisations have a duty to preserve relevant information when a lawsuit or investigation is reasonably anticipated. Staff must immediately notify the SIRO and Head of Legal Services if they have been notified of a Litigation or Investigation or have reasonable foresight of a future Litigation or Investigation as this could result in records being held beyond their identified retention period.

7.2 The Information Governance Officer will log details of the records which have been placed on hold and the justification.

7.3 The legal hold decision will be determined by Senior Leadership Board.

7.4 When a legal hold is terminated, records previously covered by the legal hold should be retained in accordance with the Information Asset and Retention Register without regard to the legal hold.

8. Intellectual Property

8.1 Intellectual Property (IP) refers to something unique that is created; for example, company names, logos, symbols, literary and artistic works.

8.2 IP enables individuals / organisations to protect designs and concepts from unauthorised re-use. An idea on its own does not constitute IP, however any documenting or development of the idea is.

8.3 IP is principally legislated under the Copyright, Designs and Patents Act 1988 and incorporates a number of different areas including:

- Copyright - Writing and literary works, art, photography, films, TV, music, web content, sound recordings
- Patents - Inventions and products, e.g. machines and machine parts, tools, medicines
- Trademarks - Product names, logos, jingles
- Designs - Appearance of a product including, shape, packaging, patterns, colours, decoration.

All research and reports; all logos or designs; all recordings verbal and/or video; photographs or images produced by members of staff for the Service, belong to the Service and remain the property of the Service even when an individual leaves the Service's employment.

Detailed guidance on how IP operates and how it is applied is available from the Intellectual Property Office.

9. Record Naming and Good Practice

9.1 Record naming is an important process in records management and it is essential that a unified approach is undertaken within all areas of the Service to aid in the management of records.

9.2 Service employees 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.

9.3 The Service standard 'naming convention' guidance is provided (refer to **Appendix A**) and should be used for the filename of all electronic documents created by Service employees from the implementation date of this policy.

9.4 The re-naming of old documents is optional but new documents must follow the standard naming convention.

9.5 Version Control is the management of multiple revisions to the same document and enables one version of a document to be identified from another. Detailed guidance is provided in Section 10 - Data Quality and Version Control of the Overarching Information Governance Policy.

9.6 All Service information is valuable and as such must be labelled with the appropriate marking to ensure the correct levels of protection are applied. Full guidance on how to classify information is detailed in the Overarching Information Governance Policy - Protective Marking.

9.7 Additionally, Service information must be stored securely whether physically locked in a filing cabinet or within the secure drive (F:drive) on Service personal computers. Information must not be saved on local drives (H:drive) or on the desktop. Further guidance is available in the Information Security Policy

9.8 Where a shared drive (F:drive) is used, it is essential that files are regularly reviewed to prevent record duplication. Service employees should ensure team members have not previously created a record prior to initiating a new document.

9.9 Good record keeping requires information to be recorded at the same time an event occurs or as soon as possible afterwards and if information is recorded by hand, writing must be clear and legible.

9.10 If information needs to be removed (redacted) from an electronic document, then a new version of the original should be made and the text deleted. This is because in Microsoft Word, text covered with the black highlight text tool can be revealed by removing the highlight. Even if the redacted document is saved in a non-alterable format e.g. PFD, it can be converted back into Microsoft Word and the text uncovered. Best methods of redaction include cover up tape, specific blacking pen and re-scanning redacted documents and saving as in a pdf format.

10. Record Maintenance

10.1 It is the Service's aim to become a largely paperless organisation and therefore staff are encouraged to save in electronic rather than hard copy format wherever possible. Original documents may be scanned and saved electronically; however large scale scanning can be a very expensive option and should only be undertaken once approved by the appropriate SLB manager.

10.2 Scanned documents / images must be of the same quality and standard of the original, so that they may be accepted as evidence by the courts where necessary. To ensure compliance, the code of practice for evidential weight and legal admissibility of electronic information (BS 1008) should be adhered to.

10.3 Paper records must be held in a shared location and the movement / transfer of hard copies should be controlled to ensure that a record can be easily located and retrieved at any time.

10.4 Hard copy files must be kept secure in accordance with the Information Security Policy and Information Asset Owners (IOAs) must ensure contingency or business continuity plans are in place to provide protection for records which are vital to the continued functioning of the Service.

10.5 Records held in electronic format and saved on shared drives, (F:drive or SharePoint) have regular back-up copies scheduled and undertaken on a daily basis by the ICT Department.

11. Record Disclosure

11.1 There are a range of statutory provisions that limit, prohibit or set conditions for the disclosure of records to third parties.

11.2 Only certain staff members have the authority to disclose records. Service information should only be shared with other organisations where an authorised Information Sharing Agreement is in place (refer to the Overarching Information Sharing Protocol), which will detail what information is being shared, who it is being shared with, why it is being shared, relevant legal justification and management approval. Personal information must only be shared in accordance with the Service's Data Protection Policy.

12. Record Closure

12.1 Records should be closed, for example, made inactive and transferred to secondary storage as soon as they have ceased to be in active use other than for reference purposes.

12.2 The Service's Information Asset and Retention Register details how long records should be kept for and whether to dispose or archive data once it is no longer required.

13. Record Appraisal

13.1 The purpose of the appraisal process is to ensure the records are examined at the appropriate time to establish whether or not they are worthy of permanent archival preservation, whether they need to be retained for a longer period as they are still in use or whether they should be destroyed.

13.2 Appraisal guidance is available from the Information Governance Officer

13.3 Where a member of staff is transferring to another Station / Department or leaving the organisation, it is the responsibility of that staff member and their Line Manager to ensure that all Service records remain or are returned to the relevant Station / Department. Any non-work related records should be disposed of.

14. Record Transfer

Records selected for archival preservation and no longer in regular use should be transferred to the Service's secure archive facility at Operational Logistics. The records remain the responsibility of the IAO regardless of location and as such it is essential that the Information Asset and Retention Register is maintained and records managed in accordance with the Register's requirements.

15. Record Disposal

15.1 Once an appraisal has been conducted, a record may be disposed. Disposal can mean the permanent archiving of data, the transfer of custody of records or movement of records from one system to another. It could also mean the destruction / deletion of the record.

15.2 The accounts (mailbox and personal folder) of staff members who have left employment with the Service will be deleted immediately unless there are extenuating circumstances, for example, an Employment Tribunal claim or litigation case. This will ensure best utilisation of server space, as well as to ensure that records are not held in excess of their retention period. It is the Line Manager's responsibility to notify the ICT Helpdesk of accounts that should not be deleted.

15.3 Short-lived documents such as telephone messages, notes on pads, post-its, e-mail messages, etc. do not need to be kept as records. If they are business critical they should be transferred to a more formal document which should be saved as a record.

15.4 Records should be disposed of in a timely fashion in accordance with Section 9 - Records Management and Disposal of the Overarching Information Governance Policy.

16. Records Security

16.1 All Service information must be labelled with appropriate protective marking levels and saved with relevant security measures. Where information is of a sufficiently sensitive nature, data should be stored in a secure drive (F:drive). Staff requiring such levels of security should contact ict@hwfire.org.uk to request a secure folder.

16.2 Staff must not use home email accounts or private computers to hold or store any official Service records or information.

16.3 Removable media must be Service owned and encrypted by the ICT Department. Ideally, personal sensitive data should not be stored on any removable media; however if there is no other option, this data must be stored on a Service encrypted device and deleted once transferred to identified secure area folder.

16.4 When printing paper records, especially sensitive documents, ensure appropriate measures have been taken in collecting all documents immediately after printing. Use "Follow-Me" facility when printing to a central printer to ensure the document is only printed when a staff ID fob is swiped on the printer.

16.5 Computers must be kept secure and access restricted to authorised users only. All staff are required to adhere to the ICT Acceptable Use and the Data Protection SPI's.

16.6 The SIRO is responsible for ensuring that all staff and managers are aware of security policies and that they are observed. Managers need to be aware they have a responsibility to ensure staff have sufficient, relevant knowledge concerning the security of information and systems.

16.7 Designated owners of systems, who have responsibility for the management of ICT systems and inherent information, need to ensure that staff have been made aware of their responsibilities toward security. IAO's need to ensure they uphold the security policies and procedures and that staff complete any relevant training.

17. Monitoring Policy Compliance

17.1 All staff and those working on behalf of the Service are expected to adhere to relevant policies. Any employee found to have breached Service policy may be subject to disciplinary procedures. Other users may have their contract terminated.

17.2 If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s). If further guidance is required on the implications of this policy or how it applies, please seek advice from the Head of ICT or the Information Governance Advisor.

18. Governance and Approval

This policy and the commitment to information security management is subject to continuous, systematic review and improvement. This Service wide policy will be governed by the SLB and the SIRO.

Appendix A: Service Electronic Document Naming Convention

These guidelines have been prepared in order to assist with arranging and naming electronic folders and files (individual documents) consistently to make it easier for staff to find electronic records but also to help with the identification of records to be deleted, preserved for the medium term or archived.

All staff are asked to adhere to these naming conventions as they are the key to maintaining well organised records. Feedback on these guidelines is welcomed; Please let the Information Governance Team know what works well and what areas need developing.

Folder and File names should be short but clear

Please avoid the use of initials, non-standard or uncommon abbreviations, codes or personal acronyms. Stick to letters (A-Z or a-z) and numbers (0-9). Avoid 'The' or 'A' at the start of file names as they do not add much to a title except to lengthen it.

Good file names	Bad file names
NamingConventionsGuidelines	The_ABC_guidnace_on_naming_conventions
2015-02-25CommitteeMeetingMinutes	Copy of Committee Meeting Minutes dated 250215

Avoid repetition and redundancy in file names

Repetition and redundancy increase the length of file names. A record should not contain information that is already present in the folder in which it is filed. However, if you are unhappy at very short titles which rely on documents being placed on the correct folder, elements may be repeated (this may be the case for committee minutes and papers).

Good folder & file names	Bad folder & file names
Folder: 2015PurchaseOrders File title: HewettRecruitment20150202 or 2015-02-02HewettRecruitment	Folder: Purchase Orders For 2015 File title: 2_Feb_15_Purchase Order To HewettRecruitment
Folder: PolicyDocuments File title: RecordsManagement	Folder: PolicyDocuments File title: Policy on Records Management
Folder: BuildingsCommittee File title: 20151002Agenda *or* 20151002BuildingsCommitteeAgenda	Folder: Buildings Committee File title: Agenda for the 2nd Oct Meeting

Date and Number Formats

To maintain chronological order use the formula YearMonthDay. Years should be expressed fully as four digits, months and days as two digits.

Good file names	Bad file names
2015-05-31-FRSCommitteeAgenda	31st May 15 Agenda for FRS Committee
20150312BusinessPlan	12Jan 2015 Business Plan
2011-03Invoices	Mar 2011 Invoices

And remember to include a leading zero for numbers 0-9. Use 02 rather than just 2.

Use Capital Letters to delimit words, rather than spaces or underscores

Some software packages have difficulty recognising files names with spaces. Using spaces and underscores also lengthens the file name. Where capitalised common acronyms are used in file names, the acronym should appear in capitals as well as the first letter of the word following.

Good file names	Bad file names
FRSContract	Contract_with_FRS
RiskManagementStrategyDraft	Risk Management Strategy draft version

Avoid using words like ‘draft’, ‘letter’ or ‘memo’ at the start of file names

Describe what the document is at the end of the title to facilitate ordering within the folder, allowing documents relating to a subject to sit together.

Good file names	Bad file names
BudgetDeadlineMemo	Memo on the budget deadline
BudgetDeadlinePolicy	Policy on the budget deadline
RecordsManagementPolicyDraft	Draft_Records_Management_Policy