Ethical Standards Commissioner

Commissioner for Ethical Standards in Public Life in Scotland
Thistle House
91 Haymarket Terrace
Edinburgh
EH12 5HE

RECORDS MANAGEMENT POLICY AND PROCEDURES

Date policy adopted: 01/04/2015
Date of last review: 24/02/2022

RECORDS MANAGEMENT POLICY

1. Purpose and Scope

This document outlines how employees of the Ethical Standards Commissioner (ESC should manage the documents and records generated as a result of their work.

This policy forms part of the contract of employment. Employees should bear in mind that refusal to co-operate in the application of any of our policies or procedures may be treated as misconduct and dealt with under the disciplinary procedures.

This policy applies to all employees regardless of working pattern or nature of employment contract. It will not apply to others carrying out work on behalf of ESC (agency staff, contractors etc) who will be governed by the contract under which they have been employed or contracted.

2. Policy Statement

The Commissioner fully recognises the value of records and has established records management as a key corporate function.

In view of the scale of this office's operations, individual employees are largely responsible for the proper and effective management of the records they generate and receive. However, the Commissioner accepts strategic responsibility for these records and has allocated a co-ordinating, operational role to the Head of Corporate Services.

Given the importance of records for day to day operations, and as the corporate memory of the office, the Commissioner is committed to ensuring that policies, procedures and practices are effective, and are regularly reviewed and developed to ensure that they continue to meet our needs and obligations.

3. Implementation, monitoring and review of the policy

ESC is required, under the Public Records (Scotland) Act 2011 (PRSA), to prepare and implement a records management plan which sets out how we manage our records. This records management policy forms a key part of our records management plan. More information about our duties under the Act are available on the National Records of Scotland PRSA webpages.

Overall responsibility for policy implementation, monitoring and review lies with ESC. Everyone covered by the scope of the policy is obliged to adhere to and facilitate implementation of the policy. Appropriate action will be taken to inform all new and existing employees and others covered by the scope of the existence of the policy and their role in adhering to it. The policy will be reviewed at such times as legislation or a change to ESC policy position requires it. The policy will be made available to the general public.

4. What is a record?

In records management it is important to be clear about the difference between a document and a record.

A document is any piece of information in any form, produced or received by an organisation or person. It can include databases, websites, email messages, word and excel files, letters, memos, social media posts, MS Chat messages and audio and video recordings. Some of these documents will be ephemeral or of very short-term value and should never end up in a records management system.

Some documents will need to be kept as evidence of business transactions, routine activities or as a result of legal obligations, such as policy documents. These should be placed into an official filing system and at this point, they become official records. In other words, all records start off as documents, but not all documents will ultimately become records

Records are an important constituent of the corporate memory of an organisation.

5. The principles of good records management

The guiding principle of records management is to ensure that information is available when and where it is needed, in an organised and efficient manner, and in a well-maintained environment.

National Records of Scotland guidance states that, “Organisations must ensure that their records are:

- **Authentic**
  It must be possible to prove that records are what they purport to be and who created them, by keeping a record of their management through time. Where information is later added to an existing document within a record, the added information must be signed and dated. With electronic records, changes and additions must be identifiable through audit trails.
- **Accurate**
  Records must accurately reflect the transactions that they document.
- **Accessible**
  Records must be readily available when needed.
- **Complete**
  Records must be sufficient in content, context and structure to reconstruct the relevant activities and transactions that they document.
- **Comprehensive**
  Records must document the complete range of an organisation's business.

- **Compliant**
  Records must comply with any record keeping requirements resulting from legislation, audit rules and other relevant regulations.
- **Effective**
  Records must be maintained for specific purposes and the information contained in them must meet those purposes. Records will be identified and linked to the business process to which they are related.
- **Secure**
  Records must be securely maintained to prevent unauthorised access, alteration, damage or removal. They must be stored in a secure environment, the degree of security reflecting the sensitivity and importance of the contents. Where records are migrated across changes in technology, the evidence preserved must remain authentic and accurate."

6. Our records management system

ESC does not retain paper records. Paper records are only generated to assist with work in progress and are securely destroyed on the completion of tasks. Any records generated in paper format must be converted to a digital format and stored electronically.

ESC stores its records in two locations.

The main server:

Currently all records related to public appointments and corporate services and a selection of records related to standards, including prospective complaints, are stored here.

Due to the size of the organisation and the costs involved, the Commissioner does not operate an Electronic Records Management System (ERMS). Without an ERMS creating, moving and deleting records can be done without any audit trail. This means records could be misfiled and deleted without trace.

In order to minimise this risk, we manage our records using a defined file plan and records management procedures. These are designed to ensure that records are stored in a consistent manner, thereby making it easy for staff to quickly retrieve information, work effectively and efficiently and meet our statutory obligations.

The case management system (CMS):

Currently all records relating to complaints about the conduct of MSPs, councillors and the board members of public bodies and lobbying are stored here. Records relating to prospective complaints are stored in the main server.

The CMS is built using Salesforce software and supported by Arcus Global. It is a cloud-based case management system. All records associated with individual complaints and cases are uploaded to the system, stored in Salesforce data centres and accessed via the internet.

The creation, movement and deletion of records is recorded in an audit trail. Deletion of records in the CMS is not an automatic process. Identification and deletion of records must be carried out manually.

7. Employee responsibilities

The Commissioner has overall strategic accountability for records management and the Head of Corporate Services has day-to-day operational responsibility.

Each employee is responsible for ensuring the records generated or received by them are stored correctly.

Specifically, each employee is responsible for correctly storing records:

- they send to or receive from external parties
- they create
- they send to internal recipients. In most circumstances:
    - where requesting a response from a team member, they will be responsible for managing the document chain.
    - where responding to a team member, it remains their responsibility to file the resulting document chain.

If it is not clear who is saving the information, the employee should clarify this to ensure that important records are not lost.

Responsibility for filing records may be delegated to other team members in specific or all instances. The delegation must be clear and documented.

In addition to the above, managers are also responsible for monitoring the records within their assigned folders to:

- ensure records are stored in line with the file plan and these records management procedures
- identify staff training needs
- correct any misfiling
- ensure that retention and disposal schedules are met.

A review of the assigned folders should be carried out every six months.

It is essential that the records management system works smoothly and effectively. It must also be flexible enough to change when business needs require it. However, changes must be undertaken in a methodical way.

If an employee considers a records management procedure or an element of the file plan is inappropriate or if they have any other concerns these should be reported to their line manager or the Corporate Services Team.

RECORDS MANAGEMENT PROCEDURES

8. General Principles

a. When saving a document always consider if a new staff member could easily find it.

b. Records must be filed by function, subject or topic, with sub-folders by activity, external organisation, date etc. For example, a letter from COSLA:
   - about the Members' Model Code of Conduct should be filed in the Member's Model Code of Conduct folder
   - inviting us to a conference on Freedom of Information should be filed in an outreach folder in the Freedom of Information folder
   - inviting us to give a talk about public appointments should be stored under Appointments Outreach Activity.

The above applies where the document sits with other associated records. Where there are no associated documents, the item and our response can be stored in the general external communication folders – *Office/Administration and Communication/YY-YYYY/Comms with external bodies*. Prior to saving, assess whether the item is a 'record' that should be saved or a 'document' that can be deleted.

Research, tenders, contracts and consultations should also be stored by topic e.g. a tender for IT services should be stored in the ICT folders, not in a generic ESC Tenders folder.

9. File plans

The main server

Records related to public appointments and corporate services and a selection of records related to standards are stored on the main server. Records are grouped together, by function, in folders. The top level folders are:

Function	Server Location	Manager Responsible
Appointments	p:\	Public Appointments Manager
Office	o:\	Head of Corporate Services
Standards	s:\	Senior Investigating Officer

The top three levels of the folder structure form our file plan and are fully laid out in the document – 'ESC File Plan and Retention Schedule'.

In order to maintain consistency and ensure our file plan reflects our records retention and disposal procedures, these levels cannot be amended, added to or deleted without discussion with the Corporate Services Team.

Folders in level 4 onwards may be added or deleted as required. Sub-folders are an aid to locating records and can be used to drill down into the topic.

The top three levels should only contain folders. There should be no unattached free-floating documents on these levels.

The Case Management System

As described in item 6 above, records relating to complaints about conduct and lobbying are stored in a cloud-based case management system (CMS). These records are stored in line with our File Plan and Retention Schedule, this policy and its appendices. The responsible manager is the SIO.

KnowledgeHub

ESC shares documents, views and information with a group of consultants (Public Appointments Advisers - PAAs) who work with us on a regular basis. Key documents are shared with PAAs using a private forum on KnowledgeHub, a secure online cloud-based collaboration tool. Private forums are accessible by invitation only.

Rules of use make it clear that information held in the shared space:

- should not contain the personal data of third parties
- could be requested under subject access and FOI requests.

The rules of use should be circulated to any users prior to their joining the forum.

These records are stored in line with our File Plan and Retention Schedule, this policy and its appendices. The responsible manager is the PAM.

Microsoft Teams

ESC uses Microsoft Teams as an office-wide communications tool.

- The Teams and Files elements are not to be used.
- The Calendar option is linked to and records managed through each user's MS Outlook profile.
- Employees may use the video and audio call functions to contact others both inside and outside the organisation. Calls should not be recorded.
- Employees may use the Chat function with other ESC employees. The following rules of use apply:
  - Employees should not share any personal data on Chat. Messages on Chat are subject to data protection and FOI legislation. This means we must have a lawful basis for keeping it, store it securely and be able to delete and correct it. We may need to examine messages when responding to information requests.
  - If sharing information, advice, hints or tips on Chat employees should ensure that individuals cannot be identified. This particularly applies to external parties but can also apply to sensitive material about staff members.
  - Employees should not share links to internal material on Chat. Links to publicly available, external material are appropriate.
  - Chat messages are automatically deleted one month after creation.

10. Records management procedures

Access and permissions

In order to ensure information is shared as effectively and efficiently as possible and records stored in the correct location, ESC allows employees access to all documents unless there is a specific reason to restrict access.

Members of the Senior Management Team and the Business Officer have full access to all drives, folders and files. Full access allows all files and folders to be viewed, created, deleted and amended.

All other employees also have full access to all drives, folders and files with the exception of o:\Staff\Personnel Files and o:\Finance\Payroll. These folders are visible but there is no access to the content.

Employees are given access to the CMS and KnowledgeHub depending on the requirements of their role.

Full details about the access permissions in place can be found in the Staff IT Permissions Register.

Naming conventions

1. Include the date, the name of the correspondent (if applicable) and an indication of the subject in the filename, e.g. 2014-08-15 BloggsJ (FOI request).msg
2. Keep file names short, but meaningful
3. Avoid unnecessary repetition and redundancy in the file-path
4. Order elements in the filename appropriately
5. When including a number always give it as a two-digit number
6. Write dates back to front and in standard formats
7. When referring to an individual, use surname followed by initials
8. Avoid common words, such as ‘Draft’, at the start of filenames
9. Avoid using non-alphanumeric characters, such as %, $ and £, in file names
10. Version numbers - the version number of a record during drafting stages should be indicated by the inclusion of ‘V’ followed by the version number (two-digits) and, where applicable, ‘Draft’ or ‘FINAL’.

Further details and examples of each rule are given in Appendix 1.

Documents generated by other organisations

Employees should be cautious about saving documents generated externally, e.g. Standards Commission for Scotland annual reports. Consider whether an external document should be saved with ESC’s records. The most up-to-date version of these documents will be available from the external body either online or on request. If a document is frequently referred to a desktop shortcut to the URL can be used.

Personal data and special category personal data

Personal data and special category personal data can be revealed in the name of a record or folder thus breaching data protection legislation. Staff members should be careful to consider this when naming folders and files and to avoid the inclusion of sensitive personal data in file and folder names where possible.

Equally do not use 'Confidential' or 'Top Secret' in a record or folder name as it merely draws attention to it.

Avoiding duplication

Records should only be stored in one location. On occasion it may be helpful to view a record from two locations. If working in the main server, first decide on the primary location and then add a 'shortcut' to this in the secondary location. Staff members should be cautious when doing this as when the original document is deleted the shortcut will remain resulting in a broken link and inconsistent disposal of records.

Email management

Email is our primary tool for communicating information. An email is no different from any other record and should be treated with the same consistency.

Emails left in mailboxes are of limited use to the wider organisation, not only in terms of conducting business operations, but because they remain inaccessible and cannot be managed corporately. However, staff members should be aware that these emails are still subject to the Freedom of Information (Scotland) Act and data protection legislation. Capturing emails into the main filing structures helps to place this information in context with other related records. It also ensures that all records, irrespective of format, are retained and disposed of in line with our Retention Schedule.

As with other types of correspondence not all emails are records. Each staff member must distinguish between the emails they need to capture for business purposes and ephemeral communications which should be deleted promptly.

The following checklist outlines how to manage emails. More detailed guidance is available in Appendix 2.

Do:

- Remember that all work emails are records belonging to ESC
- Exercise the same degree of care and professionalism in regard to the content as you would give to a letter
- Use short, meaningful titles/subjects for your emails
- Remember that all your emails may be open to scrutiny
- Remember that email is not a secure form of communication; consider whether its contents be encrypted or password-protected
- Use links to records, shared folders, drives and websites rather than sending an attachment
- When replying to an email, keep the original text as part of your response, ensuring that no personal data is accidentally revealed
- File important emails promptly so that they are accessible to other people
- Delete unwanted emails as soon as they are no longer required
- Ensure that your deleted items are actually deleted

- Set up a separate folder for your personal emails
- Use the junk mail and focussed/other filters
- Use distribution lists to avoid long 'to' lists and to avoid disseminating the email addresses of external contacts
- Set an out of office message giving alternative contact details when you are away for more than a day, or arrange for someone else to check your email

Don't:

- Use email to gossip or let off steam
- Use RE: and FW: at the beginning of a filename
- Mix personal and work emails
- Address more than one topic in one email
- Annotate or change the text of the original email when replying to it
- Use symbols in the subject line of emails
- Use emojis in formal documents
- Keep the only copy of important emails in your mailbox
- Allow backlogs of unwanted emails to accumulate in your account
- Copy emails to people unless they need to see them
- Use a non-ESC email account for ESC business (see also the Information Security Policy).

Mailbox size

To ensure that emails are being transferred promptly to the main folders, there is a size limit on your mailbox. The Corporate Services Team can inform you what this limit is. You will receive an automatic warning when your mailbox is close to this limit. You will have to decide which emails are ephemeral and can be deleted at once and which are records and need to be moved to the main filing structure.

Email formats

In order to preserve the email in a way that ensures it retains its characteristics, metadata and attachments, all emails should be saved in Outlook Message Format (*.msg). On occasion, emails may be grouped together and saved as an Outlook Data File (*.pst) file. For example, distribution emails for the annual report. Emails can also be converted to PDF format if redaction is required.

Email strings/threads

When dealing with long email chains, provided that the chain has not been edited and all the previous emails are part of the chain, it is sufficient to keep the last email in the chain and to destroy the others. However, bear in mind that attachments are stripped out when replying to emails so ensure that these are captured appropriately. If the email chain covers a protracted period of time, it will be helpful to regularly file copies. This allows colleagues to easily access documentation about an ongoing issue. Similarly, it may be helpful to file an interim copy of the email chain when a key event occurs.

Employees' personal data

Employees may keep personal data such as copies of timesheets, absence requests, leave requests or appraisals in their h:\ drives. Only genuinely personal information should be stored in these drives. They should not be used for storing business records. Employees should be aware that any data relating to ESC business held in this drive is subject to the Freedom of Information (Scotland) Act and data protection legislation. To encourage staff members to store business records in the main drives, personal drives are restricted in size. If a staff member needs to store business records of a sensitive nature and requires access to be limited they should contact their line manager who can review the request and arrange for the folders to be set up if necessary.

Line managers will ensure that any personnel records are stored in the employee's personnel file.

Review and Disposal

Most of ESC's records are not kept indefinitely, but for a set period of time. The retention period for each type of record is outlined in the File Plan and Retention Schedule.

Review arrangements

At least every six months the person responsible for the folder (the folder manager) will review it to ensure the contents are stored in line with these procedures. The folder manager will arrange to re-name or re-file any incorrectly stored records as appropriate and identify training needs. The folder manager will also arrange for the disposal of records in line with the ESC's retention schedule.

Disposal and archiving arrangements

Using the File Plan and Retention Schedule, the folder manager should identify those records for disposal. The folder manager should:

- carry out a final review of the records
- move any incorrectly filed items to the correct location
- ensure that any files that should be held for a longer period are moved to the correct folder
- identify those items to be transferred to the National Records of Scotland and inform the Corporate Services Team, who will arrange transfer in line with the procedures agreed with NRS
- delete the remaining files.

Prior to deletion a screen print of those folders and documents should be taken and added to a word document. Further screen prints showing additional folders and documents can be added as appropriate. The folder manager should add a note to the head of the document providing their name, a brief outline of the documents/folders deleted, rationale for deletion and date. The final word document should be saved to the ESC Electronic Records Destruction Log folder. It may be necessary to delete personal data from the record and folder names. When deleting items in the CMS the above method can be used or the audit trail can be saved.

The folder manager may delegate the above tasks as appropriate.

Certain key records must be transferred to archive prior to removal from ESC systems. The File Plan and Retention Schedule identifies these records. ESC archives its records with the National Records of Scotland under an archiving agreement. Full details of how to proceed are providing in our Archiving Procedures.

11. Further information

More information about ESC's records management system can be found in the Records Management Plan.

Equality Impact Assessment

Does this policy comply with the general Public Sector Equality Duty (s149 Equality Act 2010)?

This policy applies to all employees. Its impact was considered when drafting. Where a disability affects an employee's ability to adhere to this policy the appropriate reasonable adjustments will be made. We consulted with all employees prior to publication to identify and address any issues.

Data Protection Impact Assessment

Have we considered any effect the policy may have on the collecting, processing and storing of personal data?

The records generated by this policy will contain personal data. Suitable retention and destruction policies are in place to manage this material.

Information Security Impact Assessment

Have we considered the impact any policy may have on our cyber-resilience?

This policy should have no impact on our cyber-resilience.

Records Management Impact

Have we considered the impact any policy may have on our ability to manage our records?

This policy underpins our ability to manage our records.

Version	Description	Date	Author
1.0	Final version	10/03/2022	Head of Corporate Services
1.1	Updated phone number	16/05/2023	Corporate Services Officer