Ethical Standards Commissioner

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

RECORDS MANAGEMENT PROCEDURES

- Date policy adopted: 01/04/2015
- Review period: Ad hoc when a change to legislation or ESC process requires it and at least every five years
- Date of last review: 27/04/2026
- Date of next review: 31/05/2031

Contents	Page No.

Ethical Standards
Commissioner

1. General principles

a. For the purposes of this policy, “document”, “record” and “material” refers to all file types and not just written text. For example, it includes images, audio and video files.

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

c. Where possible, records should be filed by function, subject or topic, then in sub-folders by date, activity, external organisation, etc.

For example, an email from COSLA should not be filed in a single, high-level ‘COSLA’ folder, it should first be filed by function and topic and then as required.

- COSLA inviting Commissioner to speak on standards at event should be filed in Standards / External Comms & Events then the relevant sub-folder(s).
- COSLA agreeing to provide staff training should be filed in Office / Financial Year / Staff and then the relevant sub-folder(s).
- COSLA responding to a consultation on our equal opportunity strategy should be filed under Public Appointments / Diversity / and then the relevant sub-folder(s).

The above applies where the correspondence 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.

Return to Contents

2. File plans

SharePoint – Files Site
Records related to public appointments and corporate services and a selection of records related to standards are stored on the SharePoint Site named “Files”. Records are grouped together, by function, in folders. The top level document libraries are:

Function	Document Libraries (Level 1)	Responsible Manager	Day-to-day management
Appointments	Appointments Databases	Public Appointments Manager (PAM)	Support Officer
Corporate Services	Office Databases Restricted	Head of Corporate Services (HCS)	Individual team member responsible for that function
Standards	Standards	Senior Investigating Officer (SIO) and/or Hearing and Investigations Officer (HIO)	Support Officers

The top three levels of the document library 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, the top three 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.

Case Management System
Records relating to complaints about conduct and lobbying are stored in a cloud-based case management system (CMS) and a SharePoint site called “Investigations Case Files”. These records are stored in line with our File Plan and Retention Schedule, this policy and its appendices. The responsible manager is the SIO and/or the HIO.

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.

- New Teams Groups or Channels should only be created by the Information Management and IT Officer (IMITO).
- The Calendar option is linked to and records managed through each user's Microsoft 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 without previous discussion with the Head of Corporate Services or IMITO. It is acceptable for a written file note of the call to be prepared and saved to the relevant case file.
- 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 with external parties. Links to publicly available, external material are appropriate.
    - Chat messages are automatically deleted one month after creation.

Return to Contents

3. 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, Human Resources, Finance, and system administrators have full edit access to all document libraries, folders and files.

All other staff will be able to access all areas bar the "Restricted" document library, which includes staff Personnel files and Payroll information.

Only system administrators can amend permissions for other users or SharePoint sites.

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
Full information on file naming rules are given in Appendix 1 – Naming conventions.

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. Doing so may be appropriate if the body's own retention schedule is shorter than our own (e.g. Standards Commission for Scotland's written decisions or superseded versions of Code guidance and advice notes). The most up-to-date version of these documents will be available from the external body either online or on request, depending on that body's own retention schedule. If a document is frequently referred to a desktop shortcut or internet browser bookmark 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.

Avoiding duplication
Records should only be stored in one location. For example, if a file is stored on SharePoint in one particular document library, but it requires to be referenced elsewhere, a link should be created to it instead. Do not create a duplicate of the file in a second location.

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.

Staff members should ensure that duplication is avoided wherever possible. For example, when an email is filed in SharePoint or the CMS remove it from the mailbox (including from outbox and deleted items folder).

Full guidance on managing email is available in Appendix 2.

Mailbox size
To ensure that emails are being transferred promptly to the main folders, there is a size limit on your mailbox. This is detailed within the ESC IT Policy and 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). Emails can also be converted to PDF format if redaction is required.

Email chains
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 may be helpful to file copies intermittently. 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 personal OneDrive. Only genuinely personal information should be stored in this area. They should not be used for storing business records. Employees should be aware that any data relating to ESC business held in OneDrive is subject to the Freedom of Information (Scotland) Act and data protection legislation. 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 annually 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
- email the IMITO requesting deletion of the selected files.

Prior to deletion the IMITO will capture a file list of any records that are to be removed. The IMITO will email the folder manager, copying the Head of Corporate Services, confirming deletion. The deletion record will be saved to the ESC Electronic Records Destruction Log folder. It may be necessary to delete or redact 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.

Return to Contents

4. Further information

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

Return to Contents

Appendix 1 – Naming conventions

Your responsibilities

You are responsible for ensuring the records generated or received by you are stored correctly.

Specifically, you are responsible for correctly storing records:
- you send to or receive from external parties or the Commissioner
- you create
- you send to internal recipients. In most circumstances:
    - where you request a response from a team member, you will be responsible for managing the document chain.
    - where you are 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, clarify this with your colleagues to ensure that important records are not lost.

You may delegate responsibility for filing your records to other team members in specific or all instances. The delegation must be clear and documented.

Return to Contents

Ethical Standards Commissioner

Rule 1: File names should include the date, the name of the correspondent (if applicable) and an indication of the subject, except where the inclusion of any of these elements would be incompatible with rule 3 (unnecessary repetition).

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

- Date of document
- Name of correspondent (sender and/or receiver – if applicable)
- Subject description - shown in round brackets (For Example).

You should normally order the elements in the same order listed above, as it is likely that documents will be retrieved by date. However, order elements in the most appropriate way, and avoid repetition.

If it is likely that a document will be emailed externally as an attachment, it is important to name the file so that its contents are clear to the other party.

When naming the sender or receiver use the organisation name. If there are multiple contacts with an organisation, follow the organisation name with the initials of the contact, forename first. If the sender or receiver is an individual use the format ‘SurnameInitials’.

Example	
Incorrect file name	**Correct file name**
/…/Complaints About Us/ EmailFromHelenThomas10Jun03.msg LetterFromJoeBloggs5Jan04.pdf LetterToHelenThomas10Jul03.docx LetterToJoeBloggs11Dec03.docx LetterToJoeBloggs5Dec03.docx	**/…/Complaints About Us/** 2003-06-10 ThomasH (C) - ESC (Complaint).msg 2003-07-10 ESC - ThomasH (C) (Response).docx 2003-12-05 BloggsJ (C) - ESC (Complaint).docx 2003-12-11 ESC – BloggsJ (C) (Ack).docx 2004-01-05 ESC - BloggsJ (C) (Response).pdf

Explanation:
If filed correctly, all the correspondence with Joe Bloggs appears together in chronological order. The same is true of the correspondence with Helen Thomas. You don’t need to include a fuller indication of the subject, as it’s given in the folder name.

Example	
Incorrect file name	**Correct file name**
/…/Complaints/ Appeal/ WilliamEvans15Aug04.pdf WilliamEvans25Oct04.docx WilliamEvans5Aug04.pdf	**/…/Complaints/ Appeal/** 2004-08-05 EvansW (Appeal).pdf 2004-08-15 ESC - EvansW (Ack).pdf 2004-10-25 ESC - EvansW (Response).docx

Explanation:
If filed correctly, all the correspondence is listed in chronological order, it is easy to see what the correspondence is about, who it is with and its progress.

Multiple emails on the same day
If more than one email is received from the same person, on the same day, on the same subject but the latest email does not include the whole string of the correspondence, then save both emails and amend the subject element of the file name to differentiate them.

Appendix 2 gives guidance on managing your emails and when and how to save your emails to SharePoint/CMS.

When filing in the CMS the format of the record (email, letter, etc) should be included in the filename. The CMS does not allow all formats to be previewed, such as email .msg files. Including the format indicates whether preview is possible or whether the document must be downloaded to see the contents.

Records relating to conduct complaints also include a letter to indicate the correspondent type. For example:

- C – complainer
- R – respondent
- MO – Monitoring Officer
- CE – Chief Executive

Example
Correct file name
2021-03-29 BloggsJ (C) (Initial Complaint) 2021-03-30 Email chain BloggsJ (C) and ESC (acceptance of complaint) 2021-04-27 Email ESC to BloggsJ (C) (accept for investigation) 2021-04-27 Email ESC to BrownB (MO, cc CE) (initial notification) 2021-04-27 Email ESC to SmithA (R) (initial notification) 2021-04-27 Letter ESC to BrownB (MO, cc CE) (initial notification) 2021-04-27 Letter ESC to SmithA (R) (initial notification)

Case records stored in the SharePoint “Investigations Case Files” site should use standard naming conventions.

Return to Contents

Rule 2: Keep file names short, but meaningful

It is more difficult to identify a record if the file name is long.

Long file names also mean long file paths. These can cause problems in accessing the file. If the full file path exceeds the maximum number of characters permitted, then it will become inaccessible on the system.

Avoid using initials, abbreviations and codes that are not commonly understood.

Example	
Incorrect file name	**Correct file name**
Final version of the performance management policy as agreed.docx	Performance Management Policy.docx
MinutesoftheInvestigatingOfficers meeting28052014approved.docx	2014-05-28 IO Meeting (Minutes) APPROVED.docx
JBloggsHMRC(QueryRePAYESttmentfor organisationandresponse)03-04-07.docx	2007-04-03 HMRC (PAYE Statement query and response).docx

Explanation:
Some words, like ‘the’ and ‘of’ add length to a file name but do not contribute towards the meaning. If the remaining file name is still meaningful, these elements can be removed. Where words have standard abbreviations, for example ‘IO’ for ‘Investigating Officer’, these can be used in the file name.

Return to Contents

Rule 3: Avoid unnecessary repetition and redundancy in file names and file paths.

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

Example

Incorrect file name
/.../ Senior Management Team Meetings / 2014-04-30 Senior Management Team Meeting Minutes.pdf
/.../Investigating Procedures/Investigation Procedures Councillors.docx

Correct file name
/.../Senior Management Team Meetings/2014-04-30 Minutes.pdf
/.../Investigating Procedures/Councillors.docx

Explanation:
In the first example, the folder is called ''Senior Management Team Meetings' so you don't need to include the words 'Senior Management Team Meetings' in the file name. In the second example, the folder is called 'Investigating Procedures' so it is not necessary to include the word 'Investigation Procedures' in the file name.

However, if it is likely that a document will be emailed externally as an attachment, it is important to name the file so that its contents are clear to the other party.

Return to Contents

Ethical Standards Commissioner

Rule 4: Order the elements in a file name in the most appropriate way to retrieve the record.

The naming convention outlined in Rule 1 is standard. However, there may be occasions when this is not the most appropriate way to name a document.

Sometimes, the elements to be included in a file name should be ordered according to the way in which the record will be retrieved during the course of everyday business. This will depend on the way you work. If you are saving to an existing folder and are not sure which filename to use, review the filenames of the documents already stored in that folder.

For example, if the records are retrieved according to their date, the date element should appear first. If the records are retrieved according to their description, the description element should appear first.

Example	
Incorrect file name	**Correct file name**
/…/Management Team Meeting/ Agenda 1 Feb 2005.docx Agenda 20 Jan 2005.docx Agenda 30 June 2004.docx Minutes 1 Feb 2005.docx Minutes 20 Jan 2005.docx Minutes 30 June 2004.docx	**/…/Management Team Meeting/** 2004-06-30 Agenda.docx 2004-06-30 Minutes.docx 2005-01-20 Agenda.docx 2005-01-20 Minutes.docx 2005-02-01 Agenda.docx 2005-02-01 Minutes.docx
/…/Staff/Terms and Conditions 2010-11-17 Dignity at Work Policy.docx 2010-11-22 Confidentiality Policy.docx 2011-02-23 Attendance Policy.docx 2011-02-23 Code of Conduct.docx 2014-08-06 Data Protection Policy.docx	**/…/Staff/Terms and Conditions** Attendance Policy Feb 2011.docx Code of Conduct February 2011.docx Confidentiality Policy November 2010.docx Data Protection Policy Aug 2014.docx Dignity at Work Policy Nov 2010.docx

Explanation:
The first example shows minutes and agenda for Management Team Meetings. Minutes and papers of a meeting are likely to be retrieved on the basis of the date of the meeting, it is therefore best to have the date at the start of the file name, otherwise all the Agendas will come at the top of the directory list, followed by all of the minutes, and then by the papers.

The second example shows the file names of the documents in a Staff Terms and Conditions folder. Because these are likely to be retrieved by the name of the policy rather than the date, it is most useful to have that element first.

Return to Contents

Rule 5: When including a number in a file name always give it as a three-digit number (unless it is a year or a number with more than three digits).

The file directory displays file names in alphanumeric order. To maintain the numeric order it is important to include two leading zeroes. This helps to retrieve the latest record number.

Example	
Incorrect file name	**Correct file name**
FOI Response 1.pdf	FOI Response 001.pdf
FOI Response 10.pdf	FOI Response 002.pdf
FOI Response 11.pdf	FOI Response 003.pdf
FOI Response 2.pdf	FOI Response 004.pdf
FOI Response 3.pdf	FOI Response 005.pdf
FOI Response 4.pdf	FOI Response 006.pdf
FOI Response 5.pdf	FOI Response 007.pdf
FOI Response 6.pdf	FOI Response 008.pdf
FOI Response 7.pdf	FOI Response 009.pdf
FOI Response 8.pdf	FOI Response 010.pdf
FOI Response 9.pdf	FOI Response 011.pdf

Explanation:
This example shows the successive responses to a Freedom of Information request. If three-digit numbers are used the latest version will always be at the bottom or top of the list.

Return to Contents

Ethical Standards
Commissioner

Rule 6: If using a date in the file name always state the date 'back to front', and use four digit years, two digit months and two digit days: YYYY-MM-DD or YYYY-MM or YYYY.

Dates should always be presented 'back to front', that is with the year first (always given as a four digit number), followed by the month (always given as a two digit number), and the day (always given as a two digit number).

The exception is when representing a period covering two years, such as a financial year. This should be shown in the format YYYY-YY (2014-15).

Giving the dates back to front means that the chronological order of the records is maintained when the file names are listed in the file directory. This helps when trying to retrieve the latest dated record.

Example	
Incorrect file name	**Correct file name**
1Aug2005 Agenda.docx	2004-03-24 Agenda.docx
1Aug2005 Minutes.docx	2004-03-24 Minutes.docx
1Feb2006 Agenda.docx	2004-03-24 Paper A.xlsx
1Feb2006 Minutes.docx	2005-08-01 Agenda.docx
24March2004 Agenda.docx	2005-08-01 Minutes.docx
24March2004 Minutes.docx	2006-02-01 Agenda.docx
24March2004 PaperA.xlsx	2006-02-01 Minutes.docx

Explanation:
This example shows the minutes and papers of a committee. By stating the date back to front the minutes and papers are grouped together with those from the most recent meeting appearing at the bottom of the list.

Return to Contents

Rule 7: When including a personal name in a file name give the family name first followed by the initials.

It may be appropriate to include within a file name the name of an individual, usually when the record is a piece of correspondence. The family name should be given first followed by initials as it is most likely that the record will be retrieved according to the family name of the individual.

Example	
Incorrect file name	**Correct file name**
/.../Invitations Issued 2004-12-01/ SamRBrown20041201.docx	**/…/Invitations Issued 2004-12-01/** BrownSR.docx

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

There are a number of options when recording both the organisation and the individual or department in the filename.

Examples

Correct file name
2021-12-01 SPCB – AESC (Agenda for 10Dec21).docx
2021-12-01 SPCB CrerarJ – AESC (Agenda for 10Dec21).docx
2021-12-01 SPCB JC – AESC (Agenda for 10Dec21).docx
2021-12-01 SPCB – IB (Agenda for 10Dec21).docx
2021-12-01 SPCB – BruceI (Agenda for 10Dec21).docx
2021-12-01 SG – AESC (Agenda for 10Dec21).docx
2021-12-01 Scottish Government PAT– AESC (Agenda for 10Dec21).docx
2021-12-01 SG Procurement – AESC (Agenda for 10Dec21).docx

All of the above are acceptable. The context will advise the best naming convention to use. The date, name of the external organisation and subject are essential. The external party's name can be abbreviated where the abbreviation is in common usage.

It is advisable with contacting large organisations, such as the Scottish Government, to include the department or individual's name.

Return to Contents

Ethical Standards
Commissioner

Rule 8: 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.

You may only use this rule if starting file names with these sorts of words aids the retrieval of the records. See rule 4 for further details.

Example	
Incorrect file name	**Correct file name**
/…/Annual Accounts 2013-14/ Draft Annual Accounts 2013-14.docx Draft Budget Report 2013-14.xlsx Final Annual Accounts 2013-14.pdf Final Budget Report 2013-14.pdf Letter J Murphy.docx Letter P Fraser.docx	**/…/Annual Accounts 2013-14/** 2014-02-05 FraserP (Audit Plan).docx 2014-03-12 MurphyJ (Accounting treatment queries).docx Annual Accounts 2013-14 Draft.docx Annual Accounts 2013-14 Final.pdf Budget Report 2013-14 Final.pdf Budget Report 2013-14 Draft.xlsx

Explanation:
The file directory will list files in alphanumeric order. This means that all records with file names starting 'Draft' will be listed together. When retrieving the files, it will be more useful to find the draft budget report next to the previous year's budget, rather than next to an unrelated draft record.

Return to Contents

Ethical Standards Commissioner

Rule 9: Only use supported characters in a file name.

Filesystems such as SharePoint, OneDrive, and Windows only allow certain special characters to be used in filenames. Using unsupported special characters in a filename can cause the file to become corrupt or fail to sync.

The only special characters that may be used within any filename are:

- Hyphens -
- Round Brackets ()
- Full Stop .

Please note that a Full Stop . must only be used to indicate the end of a file name and the start of the file extension type.

Leading or trailing spaces in a filename are not permitted by SharePoint.

Example	
Incorrect file name	**Correct file name**
Smith,John:20070507.txt "Attendance.Policy"..docx Guidelines&Regulations.pdf Budget2006/07.xlsx	2007-05-07 SmithJ (Invoice query).txt Attendance Policy.docx Guidelines and Regulations.pdf Budget 2006-07.xlsx

Explanation:
Most special characters can be omitted without much loss of meaning, e.g. commas and quotation marks. Others can be replaced with alphanumeric characters, e.g. "&" and "+" can be replaced with "And" and "Plus". Hyphens can be used in place of forward slashes.

Return to Contents

Rule 10: It is important to differentiate between draft and final versions of documents.

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 versions.

SharePoint allows Microsoft Office files (Word, Excel, etc) to retain a version history and aid in collaborative editing. In general, a single Office file should be used to contain all drafts, as an audit history is kept within the file. Comments should be "resolved" and not "deleted" in order to preserve them in the version history.

When a document is finalised or to be published, it should be saved as a new word document or converted into a PDF with the version history, changes and metadata removed. The final working draft should be retained as it shows all versions, changes and comments ensuring an audit trail. The final word or PDF version can be issued externally or form the basis of future iterations.

Examples

Incorrect file name
Annrep0304_draft.docx
Annrep0304_final.pdf

Correct file name
Annual Report 2003-04 Draft.docx
Annual Report 2003-04 FINAL.pdf

Explanation:
This shows two versions of the annual report for 2003-04. The subject is written in full as it is a document likely to be widely circulated so a self-explanatory title is helpful. The draft is saved as an Office file format, and the final document is a PDF.
.

Return to Contents

Appendix 2 – Email management

Email content

1. Drafting the email

Think about what information you are communicating prior to composing an email message. Consider whether it is:

- for information only
- a request for action
- a request for information
- a response to a request.

If your email is long or complex, it is helpful to summarise the purpose and content and to highlight any action required at the beginning. This helps the recipient identify, prioritise and retrieve emails more effectively. Make it easy to respond to your message by clearly identifying (e.g. by numbering or bullets) your questions/requests.

Whatever the purpose of the email, indicate this by entering a short, clear and relevant description in the subject field. The reader should be able to determine what your message is about before opening it, as this will help them to prioritise their time.

Your email message may be widely circulated or disclosed in response to an information request under the Freedom of Information (Scotland) Act 2002, under data protection legislation or to another regulator. In view of this, please take care what you write.

Avoid using email to gossip or let off steam, including by copying the email to a large number of people. Ensure you read it before sending it, and check:

- Does it say what you want it to say?
- Is the tone of the email as you intended?
- If it were a memo or formal letter, what would you write and how would you write it?
- Is the email address correct?

Try to restrict an email to one topic, and do not mix personal and work matters in one email. This will make your email easier to file and will mean that you will not have to spend time redacting irrelevant or personal information in response to an information request.

Emails are not private or confidential and can be illegally intercepted. It is the responsibility of all employees to consider the appropriateness of using email to discuss sensitive subjects. Highly sensitive information should not be sent by ordinary email. Consider sending the information in an encrypted email or a password-protected attachment instead. Remember that whilst an email may be sent to an individual's account, the intended recipient might not be the only person who sees it.

2. Copying emails to others

Only use the carbon copy (cc) function when it is necessary. If it is used, ensure that the recipient of the "cc" is aware as to why the email is being copied to them. As a general rule, this function should only be used to send emails for information.

Staff must not use the Blind Carbon Copy (bcc) function. The official record must always include a complete list of recipients.

If you are delivering a message or information to a large group of external individuals, consider using a distribution list.

3. Attaching documents

When sharing information internally with other staff, documents should not be attached to emails, where possible. Instead, a link should be provided to the original document on SharePoint, to preserve an audit trail and allow collaborative editing.

You must not share internal links with external parties or groups as these can only be accessed by internal staff accounts. Instead, a copy of a file should be sent as an attachment.

If a large file or several files are to be sent externally, a file sharing service permitted by our Information Technology policy should be used with appropriate security measures such as password protection and automatic link expiry.

4. Email chains

Include the original text in your reply to an email as this ensures that you have a complete record. Be careful not to include unnecessary personal data if forwarding to another party. Be aware that personal data may appear earlier in the chain.

Avoid changing the content of the original email when responding. Whilst your amendments may be clear at the time, later changes to the context, email layout or the technical format in which the email is saved can cause the distinction between the original content and the changes to be lost. As a result, later users may be unable to tell the difference between the original email and the changes.

If you are involved in an email discussion, try to prevent the discussion from drifting off topic. If a new subject is being introduced, start a new email. This will make your email easier to file and will mean that you will not have to spend time redacting irrelevant or personal information if we receive an information request.

When dealing with long email chains, keep the last email in the chain and destroy the others. Ensure that all relevant emails are part of the chain. Bear in mind that attachments are stripped out when replying to emails so ensure that these are captured appropriately. This can be done by saving any email with attachments or by saving attachments received and the final email chain only. If the email chain covers a protracted period of time, it may be helpful to intermittently 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.

Return to Contents

Saving emails

1. Should an email be saved?

Whenever an email is sent or received a decision should be made about whether the email needs to be kept as a record. Decide whether to:

- delete it immediately
- move it elsewhere, such as the CMS, SharePoint or another mailbox folder
- leave the message in its present or a holding mailbox folder for deletion in the near future.

Keeping it in your mailbox means that it is inaccessible to others and makes it difficult to identify if the mailbox becomes too large.

Emails are used for a wide variety of purposes and so it is not possible to develop blanket rules about what should be deleted or kept. However, the principles are the same as for any record. If the email is about an important issue, you should save it to SharePoint or the CMS so that your colleagues are able to access it easily even if you are away from the office.

2. Who saves the email?

You are responsible for correctly storing emails:

- you send to or receive from external parties or the Commissioner
- you send to internal recipients. In most circumstances:
  - where you request a response from a team member, you will be responsible for managing the email chain.
  - where you are responding to a team member, it remains their responsibility to file the resulting email chain.

It is the responsibility of the sender of an email to decide whether or not to save the email. This is because each message has only one sender but may have many recipients.

If it is not clear who is saving the information, clarify this with your colleagues to ensure that important records are not lost. This will be particularly crucial when dealing with shared mailboxes.

You may delegate responsibility for filing your records to other team members in specific or all instances. The delegation must be clear and documented.

3. What should the filename be?

When saving the message to SharePoint, you should take the opportunity to ensure that the filename accurately reflects the content of the email and will be meaningful to everyone that needs to access the record for as long as it is needed. For example, a title such as, “Yesterday’s meeting” will quickly become meaningless and should be replaced with a new title.

4. Clearing unwanted emails

Delete ephemeral or out-of-date emails as soon as they are no longer required. Do not allow a backlog to accumulate as this becomes difficult to manage. The most efficient ways of doing this include:

- sorting by date and deleting all those over a certain age
- sorting by addressee/sender and deleting all those sent to or received from certain individuals
- sorting by subject and deleting those relating to completed business
- sorting by size and deleting large e-mails that are no longer required.

It is important to regularly review all mailbox folders and sub folders, such as “sent items”, “archive”, etc.

When an email is deleted, it is moved to your “Deleted Items” folder. An automated policy will remove any email from the “Deleted Items” folder after 30 days. This folder counts towards your mailbox size limit, so it is advisable to empty this folder manually if you have deleted a large volume of emails, or many attachments.

5. Out of office messages

If you are out of the office and unable to check your email for more than a day, you should set an out of office message that provides an alternative contact point such as a shared mailbox. It is not advisable to use auto forward functions as this could result in personal information being shared.

As well as helping to meet ESC’s legislative obligations, making appropriate arrangements will ensure that we act in a responsive and professional manner to all our stakeholders.

When writing an out of office message, try not to include important personal information, such as the fact that you will be away from home.

6. Sending or receiving personal emails

Our Information Technology policy allows small-scale personal use of our ICT, such as in an emergency. The policy also states that in some circumstances the ESC may need to access your mailbox, including any personal emails that you have sent or received.

To limit the circumstances in which your personal emails are examined, you are advised to copy such emails to your personal email address and delete them from your work mailbox as soon as possible.

7. Using a personal email account to send and receive work emails

It is strongly recommended that you avoid using a personal email account for work. This should only be done in an emergency. Please see our Information Technology policy for further details.

If you do have to use a personal email account for work, the emails you create and receive should be sent or copied to your ESC email account so that they can be added to the relevant record. In all cases, delete copies of work emails from any privately-owned device and personal email account.

Return to Contents

5. Assessments and version control

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.

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
2.0	Updated to reflect SharePoint migration, separation of policy and procedures, insert content from previous appendices, etc.	30/04/2026	Information Management and IT Officer

Return to Contents