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
APPENDIX 2

PROCEDURES FOR FILING ELECTRONIC RECORDS
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?

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 “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.

Consider carefully when using the “bcc” (blind copy) function. The official record should include a complete list of recipients. These will be shown in the sent email so this should be saved.

If you are sending your message to a long list of people or to external individuals that do not already know each other’s email addresses, rather than using “bcc” consider using a distribution list so that the full email addresses of all the recipients are not included in the message.

3. Attaching documents

Try to avoid attaching documents to your internal emails. This can lead to multiple versions of the attachment being created and circulated. Consider whether it is necessary to attach the information or whether a link is better suited. Links can be made to both internal servers and external sites.

Whether you provide a link or attach the original document, please bear in mind the need to ensure that everyone can read it. Consider whether to use a Microsoft Office format (Word, Excel, etc) or PDF.

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.

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, it is sufficient to keep the last email in the chain and to 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. 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.

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, the server 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 the shared drives 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
- 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 a shared drive, 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.

MS Outlook saves deleted items in a ‘Deleted’ folder rather than fully deleting them. The ‘Deleted’ folder can be used as a temporary backup. It is important to ensure that the content of this folder is regularly reviewed and emptied as it will affect your mailbox capacity.

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 or arrange for someone else to check your emails using the auto-forward facility.

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 Security policy allows small-scale personal use of our ICT, such as in an emergency. The policy also states that in some circumstances 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 Security 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.