Email Guidance

1. Introduction
2. Key Principles
3. Retention
4. Storage
5. Email Management

Name of Record	Email Guidance 3.0
Author	Senior Information and Improvement Officer
Owner	Chief Officer (Legal)
Date of Publication	22/10/24
Review Date	31/12/25

Version	Notes	Author	Date
0.1 - 2.4	Previous versions (see 2.4 for full list)	RM/SIIO	2009-2020
3.0	Amended intro. Added ref to the two different ways of accessing Outlook. Added refs. to the application of individual retentions. Typos and phraseology throughout. Emphasised InfoSec. Fixed or removed broken links. Added link to naming guidance.	SIIO	22/10/24

1 Introduction

The Council uses Microsoft Outlook as its email platform. This can be accessed through the desktop app or through your Teams account.

The Council's Information Technology section has produced guidance on email best practice and the Council has an acceptable use policy for electronic communications.

This guidance note lays out some key principles, looks at retention and storage of emails, and considers some other important issues in email management.

The importance of email may diminish as other communication platforms develop. In the meantime, however, email remains a core element of the way that the Council does business.

2 Key principles

- *All information and all communication, whatever media it is in, requires to be managed.*
- *Some emails have little or no long-term value; others are core records of the Council.*
- *Emails belong to the Council, and not to the individual employees who send or receive them.*
- *Every employee has a responsibility to actively manage their emails.*
- *The email system is a tool for communication, not for the long-term storage of information.*

3 Retention

There are a number of drivers for actively deciding what we should keep and what can be deleted.

Storage is an issue. Storage is expensive: it is simply not possible to store all the emails ever sent or received.

The Council has to deal with requests for information under the Freedom of Information (Scotland) Act 2002. This provides a public right of access to all the information that we hold - including emails. There have been several instances where time consuming and difficult searches have had to be carried out simply because officers kept emails long after they were needed.

There are similar access rights available to an individual under the Data Protection Act 2018 (DPA). Moreover, one of the key principles of the DPA is that the Council must not retain personal data any longer than is necessary. Each officer must give consideration to whether they really need to retain an email (and indeed anything else relating to identifiable, living individuals) any longer than it takes to deal with the particular matter in hand.

A cluttered, unstructured inbox in which everything is retained onto “just in case” soon deteriorates into inaccessible data.

Emails, like all other information held by the Council, need to be retained for as long as they are required and no longer. The Council has developed a records retention schedule, and this schedule also applies to emails.

It is important to stress that retention considerations relate to the process or function of a record, not to the record type. Therefore there is no single answer to “how long do I keep my emails?” as it is the context and content of that email which is significant and whether that content has been removed to the “official” record store.

Different types of emails, then, should be kept for different periods of time.

Unimportant, or personal emails should be actioned as required, and then disposed of. For example:

- “I’ve moved today’s meeting from 11:30 to 12:00”;
- An “all users” email advertising a function or event;
- “Thanks for doing that”;
- Posts from a “Listserve” or other mailing lists;
- Notices of online events, adverts for conferences, etc.

Such messages account for a significant percentage of all emails. They should not be considered as records at all, but simply deleted after you have dealt with them.

Significant or Business Critical. A significant number of emails are of continuing business relevance. They evidence the Council’s rights or responsibilities, show why a decision was taken, or give authority for a particular course of action. They can be vital in understanding why processes or cases developed as they did. They are likely to be referred to again and may require to be retained for a significant period of time.

Depending on the content and context of the email many will require to be retained (although not in the email system - see below).

The retention period is defined by the process of which the email forms a part: the Council’s Retention Schedule will help inform the decision on how long the email should be kept.

Many emails are of some short-term value but will not require a more formal designation as a record and storage elsewhere.

One suggestion is to set up a “3 month retention” folder. Such emails, including those of business significance which have also been saved outwith the system as described above (both sent and received), can be moved from the “inbox” or “sent mail” after they have been dealt with. On a regular basis, perhaps monthly, this folder is date-ordered and all the emails beyond the 3 month retention cut-off are deleted.

Alternatively, the Council is adopting the functionality to allow the allocation of individual retentions. This will only be available in the online version of Outlook, not the desktop app. Guidance will be available on this area in due course.

In summary

- Immediately delete, after actioning where required, trivial or transient emails.
- Save relevant emails outwith the email system either to SharePoint, the correct place in the shared drive, or to the appropriate line-of-business system and retain in accordance with relevant retention schedule.
- Delete all emails from Outlook after 3 months or by applying retention labels.

When confronted with an 'inbox full' message some users will simply 'archive' a vast chunk of their messages and store them on their desktop or elsewhere using the “Archive” function of Outlook. In this scenario not only do the emails still remain – but they are now contained within an unmanaged and inaccessible local silo. “Out of sight, out of mind” is rarely a good information management maxim, and “archiving” is the electronic equivalent of simply sweeping dirt under the carpet.

4. Methods of Storage.

Significant emails should be stored NOT in Outlook, but in the relevant line-of-business system (where relevant), in a properly structured SharePoint system, or in the appropriate area of the shared drive. This preserves the accuracy, authenticity and provenance of an email, allows it to be stored with other records relating to the same subject, and ensures proper security, access and final disposal outcome.

Emails should be stored with the other records that support that particular function. As with all other Council information, officers should avoid storing such information on their own personal drives H-drive or OneDrive, and departments should ensure that where appropriate shared drives are available, eliminating duplication, giving due regard to security, and allowing information to be properly structured.

In (the increasingly rare) circumstances where an email relates to a process which is still essentially paper-based, and where the authority record of that process is a conventional paper file, it may be appropriate to print the email off and store it in that file. The email will then acquire the same retention criteria as the other elements of that file. The electronic copy of the email can then be deleted. Increasingly, the Council would expect that information will be retained electronically but there may still be circumstances in which hard copy is appropriate.

5 Email management

The Council already offers guidance on various aspects of email use and management. This section deals with a number of related points not covered elsewhere - although note that all officers must complete the Information Security training and be aware of the threats posed here.

Dissemination of emails. It is very easy to send emails to a variety of recipients. Take care, though, not to overuse functions like “forward” and “cc”, and do not automatically “reply to all”.

Remember that you cannot guarantee that the recipient of your emails will delete them as appropriate and they can therefore become a permanent record which may be accessed through Freedom of Information or the subject access provisions of the DPA.

Always consider this before emailing on a sensitive topic and if it is not something which you would commit to a formal letter or memo, then consider whether to send the email at all.

Responsibility for email management. Every employee has a responsibility to manage their emails.
The National Archives has made some suggestions on the responsibility for an email:

- For internal email messages, the *sender* of the email, or initiator of an email dialogue that forms a string of email messages;
- For messages sent externally, the *sender* of the email;
- For external messages received by one person, the *recipient;*
- For external messages received by more than one person, the person responsible for the area of work relating to the message.

Naming conventions. Use the “subject heading” of your email sensibly. Put in enough information to allow the easy identification of the email, but do not make it so unwieldy that you duplicate the entire message. Strike a balance between brevity and accuracy. Email titles like: “Hi there”; or “a few points” will *not* aid the future accessibility and management of a record.

If emails are being stored electronically outwith the email system, consider at that stage whether the subject title is the appropriate title to assign there, or whether the title needs reformatted or further information – such as a machine readable date (yy/mm/dd) – to be included.

Consider using file references rather than a name or other personal identifier in the subject headings wherever possible.

Further guidance on naming conventions is available here.

File types. When emails are being saved electronically outwith the email system, consider the format in which they are to be stored. HTML files are small in size and versatile, but Outlook Message files are best in terms of retaining the associated metadata.

Attachments. Where a document is available on a website, or on the intranet, or in a shared area, send the URL (the “link”), rather than including a copy of the document. Large image-based files will quickly slow down the system and fill up the personal space allocations of everyone you send them to: much better to allow “point and click”. This is very straight-forward:

- open the webpage or intranet page where the document is mounted
- double click on the address line
- Select “Edit” and “Copy”
- In the body of your email select “Paste”

In this way everyone to whom you send the email can access the document – without you having created multiple copies and unnecessarily using storage space.

Deleted items. Remember that putting emails into the “deleted items” folder in Outlook does NOT actually delete them. You still have either manually empty the “deleted items folder (under “Tools”), or set your Outlook options to automatically empty your “deleted items” folder on exiting the program.

Old accounts. Once an officer has left the Council, their email account must not be left unmanaged. It is recommended that such accounts are closed six months after the officer has left the Council, and all its contents deleted. Prior to this happening it is the responsibility of the line manager to ensure that any emails of longer term value are stored at the appropriate alternative location.

See also

- Guidance on information security, in particular in relation to phishing emails: https://intranet.erc.insider/infosec (intranet)