East Lothian Council

Managing Email Policy

October 2019

1. Introduction and Purpose

East Lothian Council is committed to improving the way in which electronic documents are managed and used throughout the organisation. This policy must be followed by all staff when managing emails.

Email needs to be managed effectively in order to enable the efficient storage and retrieval of information; support compliance with all relevant legislation, including the Data Protection Act 2018, Freedom of Information (Scotland) Act 2002 and Public records (Scotland) Act 2011; and to reduce costs and pressures on the server storage.

2. Sensitive Information

It is the responsibility of all staff to ensure that personal and sensitive data is kept secure and is protected at all times. The privacy and confidentiality of information sent outside of a secure email network cannot be guaranteed, therefore, care must be taken when using email to communicate such data.

Colleagues should ensure that care is taken when sending or forwarding emails in order to ensure that sensitive and/or confidential information is not being passed on without the appropriate permissions. In particular colleagues should check the intended recipients address carefully before sending an email, as autocomplete function within outlook can result in an incorrect address being substituted for the intended recipient.

Emails containing personal information are covered by the Data Protection Act 2018 and must be treated in line with the principles outlined in the Act. Under the Act, personal information includes opinions about an individual or the personal opinions of an individual. Emails containing this type of information should only be used for the purpose for which the information was provided/collected, be accurate and up to date, and must not be disclosed to anyone out with East Lothian Council without the express permission of the individual concerned unless we have a legal basis for doing so.

3. Responsibilities for Managing Email

It is the responsibility of all staff to manage their emails appropriately. Colleagues should identify emails that are records of their business activities and transactions, move them from personal mailboxes and manage them alongside other records.

It is the responsibility of the sender of an email or the initiator of a dialogue to decide if the email and/or attachment(s) constitute an official record. If the email or its attachment(s) contain key decisions and/or actions taken, it should be considered a record, renamed, if appropriate, in accordance with the document naming conventions and saved in the most appropriate place.

If you are the sole recipient of an external email or, if there are several recipients, and you are responsible for the most relevant work area, it is your responsibility to decide if the message forms part of an official record or not and take responsibility for its management.

When managing emails in a shared mailbox, colleagues must be clear as to who's is responsible for the retention, naming, capture and disposal of emails within the mailbox. Without the identification of these clear responsibilities, emails may be lost or duplicated. It is recommended that the folder owner is the designated person with responsibility for a shared mailbox.

Emails that contain information that is not supported by fact should indicate that it is the sender's opinion that is being expressed.

4. Retention and Disposal of Emails

An emails value is based on its content, so the retention or disposal of emails should be based on the information they contain or the purpose they serve. The content of emails may very considerably, so no single retention period applies to all email. Please see the table below for further guidance.

Type of Message	Examples	Value	Retention
Transactions that provide evidence of your business activities.	Emails recording policy decisions, evidence of business transactions with stakeholders (including attachments)	Records required for ongoing business.	To be retained in accordance with the retention and disposal schedule.
Information messages with a business context but not part of a business transaction	Notifications of meetings, general circulars to staff, travel arrangement, discussions in which you were involved but another member of staff has responsibility for documenting and recording	Records of short lived value	Destroy when administrative use is concluded.

5. Capturing Emails and Attachments

In order to prevent loss of information, emails must be acted upon and moved to an appropriate location as quickly as possible.

It is not necessary to capture every email conversation string, separately. Instead email should be captured at key points during the conversation, when key decisions are made and transactions processed.

Email attachments should be saved as part of a record, in order to provide context to an email. However, there will be occasions when it won't be necessary to capture

both the email and the attachment. For example, if an attachment has been sent for reference purposes only and you know it's captured elsewhere.

When capturing emails, the Outlook Message Format (.msg) should be used in order to ensure that the saved email is a true representation of the email as a record and retains the characteristics of the original email.

If the title of an email does not reflect the content of the message then it should be re-titled at the point it is captures. Re-titling email records is particularly important when they represent different points in an email string as it will help identify the relevant aspects of the conversation.

6. Email Archiving and retention

Email services operate archiving software called Enterprise Vault this was introduced to help alleviate the strain that increasing amounts of email traffic and storage is placing on the infrastructure.

Enterprise Vault will free up space in the mailbox, improve performance and increase server reliability. It should be noted that all emails that form part of the record should be filed appropriately and in a timely manner.

Enterprise vault will scan your mailbox, determine which mail messages are older than 60 days, and move these to a vault specifically created for you to store your archived messages.

These items will be permanently deleted after they have been stored in your vault for a period of 1 calendar year.