Records Management Toolkit – Good Practice Guide: Managing email

1. Purpose

This document has been prepared as part of the University's approach to information and records management. It aims to assist with improvement in the University's management of documents and records by establishing coherent standards of practice.

It is intended to provide a common set of rules to ensure the control of paper and digital records.

This document contains guidelines that follow good practice in terms of records management and are generally recommended for use within the University. It is recognised that other protocols and systems may be in use which meet the different business needs of Offices, Schools and Departments in the University.

2. Rights & Responsibilities

2.1 Right to privacy

Individuals have a right of privacy in their personal lives, and a right to know their employer's position with regard to the monitoring of communications. As an employer, the University has the right and responsibility to ensure the quality and legality of its activities and the security of its systems.

In common with the principles for managing any University information, those using email systems should only keep emails if the message:

- Proves you have taken a particular action.
- Proves some action has been taken by another individual
- Provides the best way of keeping the information (e.g. if you want to keep a reference to a person's contact details, save the information to your contact list rather than retaining an exchange of email messages)

2.2 Scrutiny

Remember that all your emails may be open to scrutiny so create communications only for what is needed to progress an issue, and retain what is needed for proof that an action was taken.
To maintain a sufficient record of exchanges about a major issue or project you should:

- Decide what the salient records to retain are, and be rigorous about weeding out draft documents and discursive exchanges from the final selection
- Decide who will be the recognised records keeper for a particular issue – even if the emails are kept on a shared drive, one person should have responsibility for providing access to them on receipt of a request
- Emails are a form of official communication and should be written with the same care as letters or memos.
- Use your University email address for University business.
- Check the content for clarity, and to make sure that they contain nothing which will embarrass the University, make it liable to litigation, or defame an individual.
- Use meaningful subject lines, so that they reflect the content of the message accurately.
- Keep emails as brief as possible.

- In the interests of information security and saving resources, you must heed the advice on emails from IT Services.
- If possible only address one topic per email.
- Emails may have to be disclosed when requested, as evidence in cases of discrimination, harassment, or defamation.
- Information about a living individual is disclosable to them under the Data Protection Act 1998.
- General information exchanged by email may be disclosable to the public, through the Freedom of Information Act 2000.
- When replying to an email, only keep the relevant parts of the original text as part of your response, so that the context of your message is clear. As emails are potentially disclosable you need to make it clear in the reply that you had edited the original text. For example, use “>” to indicate original text.
- Set up separate folders for your personal emails and weed regularly.
- Establish a structured file directory (by subject / activity / project).
- Use folders to store messages for reference and delete any messages you no longer need
- Remember to delete your sent messages folder regularly.
- Users of MS Exchange and Outlook can delete messages without the option of recovery by selecting “Shift"+"Delete”. If you only use the “Delete” key, remember to also empty the Deleted Items/ Trash Bin regularly.
- Outlook and Exchange retain deleted items, even after you have emptied the Deleted Items folder. You can permanently delete these emails by selecting, depending on your software version, either "Folder" or “Tools”, then “Recover Deleted Items”, “Select All”, then “Purge”.
- Do not allow backlogs of unwanted emails to accumulate in your Inbox or Deleted Items folder, as this impedes your ability to locate the information you need (and reduces the speed of the server for everyone else).
- Before you send messages to individuals, understand how to use carbon copy (cc) and blind carbon copy (bcc) functions.
- Do not copy emails to people unless they need to see them, especially if the content is confidential. Make it clear to the recipient they should not pass on the message without first contacting to you (or the original sender).
- Use shared drives, servers or websites to give access to joint documents rather than sending them as attachments.
- Or, send documents as part of the email text (this can be useful when sending messages to multiple recipients “for information”).
- Be consistent about the use of sensitivity flags or security marking. Use “confidential” or “high priority” when it reflects the nature of the content rather than as a matter of routine. Be aware that use of these flags may draw attention to the message, and does not necessarily ensure confidentiality.
- Don’t create long lists of names in the “to” field -- if you regularly send messages to a group of people, IT Services can create a distribution list for you.
- Whatever your email system, don’t rely on the “Recall Message” function – this function is dependent on the way that the recipient’s server is configured, so there is no guarantee that it will work.

2.3 Security

- Ensure your computer is locked or logged out when you leave your desk, as someone else could send messages in your name.
- Never reply to unsolicited spam email, even when given an option to remove your name from their mailing list as this just a trick to confirm to that your email address is valid.
- If you subscribed to a list, then it’s safe to use the instructions given by the host.
- Keep you passwords or log-on code secure and ensure that they are not visible to the casual observer.
- Remember that email is not a secure form of communication. Emails may be sent to the wrong person inadvertently, or your communications may be intercepted. It is the electronic equivalent of sending a postcard.

- If you need to send confidential information (e.g. examination questions or results, sensitive communications) contact IT Services for guidance on encryption.
- If your role requires you to deal with large volumes of email correspondence, set an "autoreply" message giving alternative contact details when you are away.

2.4 Handling attachments

Avoid clicking on links or attachments in unsolicited emails, as this is a common way to spread computer viruses.
If other staff require access to important emails, file them in a public folder or shared drive. Contact IT Support for guidance on setting up folders or shared drive access.

3. Emails & Information Requests

Many FOI requests and Data Protection Subject Access Requests ask for information potentially held in email accounts. In the event of these requests, work email accounts – including the inbox, sent, and deleted folders – must be searched for relevant information. Any resulting emails are forwarded to the DP Officer for consideration in the final response to the applicant.

It is important for staff to note that work accounts are not the only email accounts that may be subject to search under a FOI or DP request. This means that FOI may apply to information held in a private email account, if that information relates to University business.

If you are conducting University business via your personal email account, those emails should be disclosed in the event of a FOI or DP Subject Access Request. If you know that you hold emails in your private account that are relevant to the request, it is your responsibility to provide them along with any other information relevant to the request.

Wherever possible, work-related conversations or discussion of any University business should be conducted via University email services.