

## **Managing emails as records**

This guidance is intended for every member of University staff who creates, receives or uses emails as part of their work.

This document provides brief, practical guidance on how to manage emails as records, and help comply with the requirements of data protection and freedom of information legislation.

## **Writing & sending emails**

1. Remember that all work emails are University records.
2. Consider whether a telephone call or visit in person could be more appropriate than an email.
3. Create clear and professional communications as almost all work emails could be released in response to an information request.
4. Restrict each email to a single topic; this will make it easier to file.
5. Don't mix personal and work content in an email.
6. Use shared drives, Sharepoint (SP) sites, servers or websites rather than sending an attachment.
7. Use plain text.
8. When replying to an email, keep the original text as part of your response to maintain a complete record of the correspondence.
9. Don't annotate or change the text of the original email when replying to it; this may become indecipherable in the long term.
10. Use encryption for high and medium risk information, as defined in the University guidance on encrypting devices and documents to protect University information.

- [Guidance on encrypting devices and documents to protect University information](#)

11. Use the email title to flag messages containing sensitive information.
12. When you send an email, ensure that your email system automatically saves a copy of the message, perhaps in a sent messages folder.
13. Use distribution lists to avoid long 'to' lists or to avoid disseminating the email addresses of external contacts. For external contacts, if you can't use a distribution list, then use the "bcc" (blind copy) function.
14. Don't use the "bcc" function on internal staff emails. The official record should include a complete list of those to whom the email was sent.
15. Make use of expiry date and properties options if these are available in your system.

### **Filing & deleting emails**

16. Store emails in the University email system, shared drives, or SP sites, not on your computer hard drive or device.
17. Whenever an email is sent or received, decide whether to leave the message in its present folder, to delete it immediately or to move it elsewhere.
18. Delete emails from your inbox as soon as they are no longer required.
19. Most emails are of short-term importance and do not need to be kept beyond the timeframe of the task to which they refer. Move them to a temporary folder named after the task to which they refer. Once that task is complete, delete the whole folder.
20. Save important emails so that they are accessible to other people (e.g. on a server, shared drive, shared email account or SP site) as soon as they are sent or received. Reveal any "hidden" header information before saving the email and ensure that you save the full header information whenever possible.

21. When saving emails to shared drives or SP site, save attachments as separate documents from emails. See the file naming conventions for recommendations as to how to title emails and attachments if you are saving them to a shared drive or SP site.
  - [File naming conventions](#)
22. When dealing with long email strings, provided that the string has not been edited and all the previous emails are part of the string, keep the last email in the string and destroy the others.
23. Provided your important emails have already been filed elsewhere, regularly delete all your sent items over a certain age (e.g. three months).
24. Ensure that your deleted items are actually deleted and not held in a waste bin.
25. Set up a separate folder for your personal emails.
26. Don't use an email auto-archive facility as your emails will not be accessible to others.

### **Mailbox management**

27. Don't use a non-University email account for University business.
28. Don't auto-forward all your emails to a non-University email account.
29. Don't give your password to another person.
30. Set an out of office message giving alternative contact details when you are away, or arrange for someone else to check your email.
31. Don't include important personal information in an out of office message, such as the fact that you will be away from home or that your office will be empty. An example text is, "I will next see emails on insert date. Please contact insert name & email address if you require a response before that date."

32. If you work in a high-profile role, or one that regularly generates enquiries, you may wish to set up a generic email contact address, accessible to more than one member of staff.
33. If you are leaving the University, ensure that you have saved important emails to a shared drive, SP site or another place where they will remain accessible after you have gone. Set an out of office message that gives details of a new contact point.

### **How should I go about clearing out a backlog of emails?**

34. Set up new systems to ensure that all new emails are saved, moved or deleted as they arrive or are created.
35. Identify items in the backlog that can be immediately deleted. 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 emails that are no longer required.
36. Set up a folder(s) to hold the remaining parts of the backlog. Keep them for five years. If, during that time, you access an email, save, move or delete it as appropriate. At the end of the five years, delete all the backlog emails that you have not accessed.

### **What is the definition of an important email?**

Email is used for a wide variety of purposes, so it is not possible to develop blanket rules about what should be deleted or kept. An email is important if:

- We need the information to carry out our business, such as day-to-day administrative records or material potentially relevant to present or future research.
- There is a legal requirement to keep the information.
- We need the information for financial purposes.
- We will need the information to explain why we arrived at a particular decision.
- We will need the information if our decision is challenged in court.
- We will need the information to be publicly accountable for our policies and decisions.
- We will need the information to help us deal with similar situations in the future, such as records that show what procedure was followed in a particular situation or copies of past references provided for students or staff.
- We will need the information to defend our rights and responsibilities, or the rights and responsibilities of others.
- The information has value for historical and cultural research purposes.

## **Responsibilities**

All University staff who create and receive emails have a responsibility to create appropriate records, to capture important emails in your area's record-keeping system and to destroy those emails that are no longer needed.

Unless an email has been received from a different part of the University or from an external correspondent, it is the responsibility of the sender of an email to decide whether or not to save it. This is because each message has only one sender but may have many recipients.

## Why should I manage my emails?

Your work emails are an important part of the University's records. Managing your emails will help you:

- Ensure that you can find what you want when you need it
- Ensure that your colleagues can find important information even if you are not in the office
- Save server space and make better use of resources
- Comply with data protection and freedom of information legislation.

## What have data protection and freedom of information to do with my emails?

Data protection legislation and the Freedom of Information (Scotland) Act 2002 apply to all the emails that you send and receive as part of your work.

Data protection legislation permits people to see information that the University holds about them while freedom of information gives people the right to access any other recorded information that the University holds, including in emails. Both pieces of legislation have tight deadlines which mean that the University must be able to retrieve information even if key staff are away.

Data protection legislation also requires us to hold information about living identifiable individuals for no longer than is necessary.

If the University does not comply with this legislation, it can be investigated by regulatory authorities and in certain cases could be fined, sued or held to be in contempt of court.

## About this guidance

Version control	Author/editor	Date	Edits made
18	Rob Don	21 February 2024	Revised to

			modernise.
17	Rob Don	25 January 2024	Amended broken link.
15	Claire Friend	March 2016	Reformatted for accessibility.
14	Sara Cranston	February 2018	Minor edits and formatting, addition of point about not auto forwarding emails
12	Susan Graham	June 2014	Revised and rewrote

If you require the guidance in an alternative format, please contact the Records Manager at [Rob.Don@ed.ac.uk](mailto:Rob.Don@ed.ac.uk)