Version number: 2.1
Policy owner: Su Longden, Data Protection Officer
Effective date: 01/09/2018
Review date: 01/09/2019

EMAIL AND CALENDAR POLICY FOR STAFF

Email is the primary means of communication for many staff and students at the University of Chichester. Email communication is person-to-person, but the outcome of an email exchange can have a much wider significance. For example, a member of staff could inadvertently commit the University to a contract by an email message or could cause illegal material to be transmitted through the University's systems for which the University may be liable. All emails and calendar appointments held at the University are legally discoverable following a request under Data Protection legislation or the Freedom of Information Act and may be cited as evidence in legal proceedings.

1. Underpinning principles

1.1 Appropriate management of email is essential in order to comply with legislation and avoid the known dangers of keeping too much information. A "one size fits all" approach to email retention is inappropriate in the University's environment when it comes to management of emails. Those responsible for an email account are best placed to decide what to retain and what to delete based on the needs of their department and any legal requirements or regulations specific to their area of work.

1.2 Every owner of an email account should have a policy for the archiving, retention and deletion of all emails in the email accounts for which they are responsible. This can include details of appropriate locations to save important records, such as a restricted shared folder. This policy is usually one agreed at a departmental level, and will follow similar principles to any other file retention policy.

2. Deleting Emails

2.1 If you have any emails in your inbox or email folders that were received twelve months ago or earlier, you should decide whether to

- delete the email;
- save either the entire email, or just a significant attachment, to a folder on your personal network drive;
- save either the entire email, or just a significant attachment, to your team or department's shared network drive, or a secure area on OneDrive with access to named individuals.

2.2 The criteria for your delete/save decision should include:

2.2.1 Compliance with University and department policies, normal practice and in particular Data Protection legislation.

2.2.2 Risk assessment on the likelihood that the email might be needed in the future and the potential consequences if that email is unavailable.

2.2.3 Risk assessment that you might need to search for that email and release it outside of the University as a result of a Freedom of Information Act or Data Protection Subject Access request.

2.2.4 Your department's guidelines and retention policy.

2.3 The presumption is that unless there are good reasons to retain an email, it should be deleted.

3. Saving emails

3.1 Emails deemed to be University records need to be saved and retained in line with the relevant section of the file retention policy. Care needs to be taken to ensure any email that needs to be saved is given an appropriate file name and location in order that it can be retrieved at a later date, and similarly deleted when it is no longer needed. Often it will be most appropriate to save an attachment rather than the entire email.

3.2 Individuals are responsible for managing their own network folders, and as such are advised to periodically check the contents and consider whether to retain or delete each document. This is particularly important for emails that contain personal data and are therefore subject to Data Protection legislation.

3.3 There are some email messages which are particularly important to retain and therefore their archive is managed at a departmental level. Examples include emails required for statutory audit trail purposes such as correspondence on contracts or purchases, correspondence pertinent to quality assurance processes, or evidence required by regulatory bodies. Your department should have a policy of what to be included and also details of the process of depositing messages, with file organisation and naming conventions.

4. Automatic deletion of "Deleted Items" after 12 months

4.1 When you delete an email from your inbox this is not actually "deleted", it is simply moved into your Deleted Items folder.

4.2 At the end of the 18/19 academic year, in August, **any items older than 12 months in the Deleted Items folder will be automatically removed and thereafter, on a daily, rolling basis, items older than 12 months will be automatically removed.** This is to ensure compliance with Data Protection legislation and requires all staff to ensure that only items that are no longer required are kept in the Deleted Items folder.

4.3 Staff members can also permanently delete these items themselves by emptying the folder manually as required, and in some areas of work, particularly those handling very sensitive personal information, it may well be appropriate to have a departmental policy of more frequent deletion. For more information on how to do this please consult the IT Help Pages.

5. Automatic deletion of historic "Sent Items" and Calendar appointments after 24 months

5.1 Similarly at the end of the 18/19 academic year, in August the **Calendar appointments and Sent Items of each email account will be automatically reviewed and any items older than 24 months will be deleted and thereafter on a daily, rolling basis, items older than 24 months will be automatically deleted.**

5.2 It is, therefore, essential that any significant email conversations, appointments or attachments are saved in an appropriate location without delay to ensure these are accessible when required.

6. Calendar sharing and delegate access

6.1 Every University IT account provides access to a Microsoft Outlook calendar. Please ensure you keep your online calendar up to date, showing day-to-day availability and times/days when you are away from the University so that your colleagues are able to schedule meetings with you.

6.2 By default, all users who have a @chi.ac.uk email account can see other users' free/busy calendar information. If you want to give other people additional rights to view your calendar, such as subject, location or full details, you will need to share your calendar. Data Protection legislation

requires that information is not shared more widely than necessary. To ensure that your calendar meets the requirements of Data Protection legislation:

6.2.1 Think carefully before giving full access to other users. Would free/busy be enough for the purpose?

6.2.2 Consider who has access to the full detail of your calendar before recording information in calendar appointments. Could individuals access more information than they need about others?

6.2.3 Avoid including personal data in the detail of a calendar appointment. This is particularly relevant for staff arranging potentially sensitive appointments, such as student support services.

6.2.4 Select "Private" for any appointments you create that contain more information than you wish to share with those who have full access to your calendar.

7. Security tips

7.1 Press the Win + L key combination (Win is the windows key) at the same time on your keyboard to lock your screen when you are away from your desk, to ensure that other users do not access your emails or send messages from your account.

7.2 Never forward University emails to your home email address. Refer to the Electronic Information Security policy for further information on this.

8. Good inbox management

8.1 Send hyperlinks to documents rather than attachments, to ensure that the information is held in a single location rather than in several users' inboxes and/or sent items. This helps with easy management of access as well as appropriate retention/deletion.

8.2 Avoid using email sub-folders within your Outlook inbox as these are difficult to manage and are not as securely backed up as other storage – instead, "drag and drop" the emails into the appropriate network location e.g. a restricted shared folder on the S drive.

8.3 Carefully check the auto-suggest email address when you are typing in the "To:" field, particularly when sending emails from a phone or tablet with a smaller screen, to ensure that they are addressed to the correct recipient or group before you press "send".

8.4 Review circulation lists before sending to ensure that emails are only going to the necessary recipients, and never send personal confidential information to a group email address without checking first who the group members are. If possible always use a named email address or a specific resource account for sensitive confidential emails.

8.5 Use a simple email signature that contains your contact details for both external and internal email.

8.6 Only keep emails if you have a reason to do so.

9. Email etiquette

Communication is so much more than simply the words we use; we interpret body language, facial expressions and tone of voice to help give context to the information. Clearly emails *only* contain words, and it is therefore both wise and polite to think carefully about the content and phrasing we choose. There are a few generally accepted points of email etiquette which are listed below:

9.1 Include a relevant subject line that doesn't include the names of individuals.

9.2 Try to avoid using acronyms or jargon, unless you are sure that they will be understood.

9.3 Keep your messages short, clear and to the point.

9.4 Never send personal remarks and do not reply to an email when you are feeling angry as you may regret it later.

9.5 If you expect there to be a delay of more than a few days before you fully respond to an email, consider sending a brief acknowledgement to let the sender know you have received their email and are not ignoring it.

9.6 Tell your correspondent if you forward a message on to someone else, so they know who will reply.

9.7 Don't use CAPITALS as it is considered to be SHOUTING

9.8 Use the "High Importance" flag if relevant, but do not overuse this or it loses its impact.

9.9 If an email has been sent to a large group of individuals, think very carefully before selecting "Reply All" to help minimise the number of unnecessary emails in your colleagues' inboxes. If you access your emails through a web browser the default option will be "Reply all", but it is very easy to change the default setting to "Reply" – click for guidance on the IT Help pages.

9.10 Set an 'out of office' reply to your email account when you will be away from work to include the duration of your time away (including start and end dates) and who should be contacted during your absence. Ensure that the named contact is available during your absence, and consider also including the SIZ helpdesk contact details help@chi.ac.uk.

10. Further information

For the most recent guidance and policy relating to privacy and Data Protection, including advice on determining your departmental retention policy, please visit the pages on the intranet https://staffnet.chi.ac.uk/data-protection/content/guidance-and-policy.