|  |  |  |
| --- | --- | --- |
| Version number: | 3.0 |  |
| Policy owner: | Su Longden, Data Protection Officer |
| Effective date: | 28/06/2022 |
| Review date: | 27/06/2024 |

EMAIL, INSTANT MESSENGER, AND CALENDAR POLICY FOR STAFF

**1. Principles and scope**

* 1. This policy outlines the standards you must observe when using the University’s email and related services, systems, and facilities. These standards are designed to minimise the risks that the inappropriate use of email exposes the University to. It sets constructive guidelines on the use of email at work (wherever located) for the smooth and efficient running of the business.
  2. Compliance with this policy is mandatory for all employees, in line with each employee’s contract of employment. It is also binding on all other users of the services mentioned, including (without limitation) governors, contractors, and visitors. All staff are contractually required to stay up to date with, and comply with, all University policies, and failure to do so may result in disciplinary action. This policy may be updated at any time and any significant changes will be communicated to all users.
  3. By making use of the University’s email facilities and related services, you assume responsibility for your compliance with this policy, without exception, and those Acts, Policies and Regulations referenced therein and enacted or authorised by the University and other regulatory bodies. It follows that you have a duty to practice appropriate and proper use of email facilities, and understand your responsibilities in this regard.

**2. Related documents/policies**

2.1. [Electronic Information Security Policy](https://www.chi.ac.uk/about-us/policies-and-statements/it-information-and-web)

2.2. [IT Privacy and Monitoring Policy](https://help.chi.ac.uk/privacy-and-monitoring)

2.3. [Staying Safe Online](https://help.chi.ac.uk/staying-safe-online)

2.4. [University Privacy Standard and associated Privacy Notices](https://www.chi.ac.uk/about-us/policies-and-statements/data-protection)

* 1. [University Records Retention Schedule](https://www.chi.ac.uk/about-us/policies-and-statements/data-protection)
  2. [Disciplinary Policy and Procedure](https://www.chi.ac.uk/about-us/policies-and-statements/employment)

**3. Legal**

3.1. Although email is a vital business tool, which we use day to day for person-to-person communication, 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 email message, or could breach confidentiality. You should consider the following legal points before sending or deleting an email, no matter who the recipient is.

3.2. You must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, pornographic, or otherwise inappropriate emails. Anyone who feels that they are being harassed or bullied, or is offended by an email received from a colleague, should inform their line manager.

3.3. You should take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract. Remember that normally you have no control over where your email may be forwarded by the recipient. Avoid saying anything that would cause offence or embarrassment if it was forwarded to colleagues or third parties, or found its way into the public domain.

3.4. The information contained in emails may be confidential to individuals or the business. A breach of confidentiality or loss of data could be considered as gross misconduct which may result in an employee being subject to a disciplinary process.

3.5. Email messages are required to be disclosed in legal proceedings in the same way as paper documents. Deletion from a user’s inbox or archives does not mean than an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable, either from the main server or using specialist software.

3.6. Email messages may be disclosed where individuals make a request under the Freedom of Information Act 2000. You must not alter, delete or destroy any information that has been requested by someone to prevent them from gaining access to it. To do so would constitute a criminal act and would be in breach of this policy.

3.7. Email messages may contain information governed by Data Protection Legislation, being all applicable data protection and privacy legislation in force in the UK including the UK GDPR and the Data Protection Act 2018. Email may be disclosed where individuals (staff, students, or anyone else) make a Subject Access Request to the University. As with paragraph 3.6 above, you must not alter, delete or destroy any information that has been requested by someone to prevent them from gaining access to it.

**4. Acceptable use**

4.1. The University's main purpose in providing IT facilities for email is to support the teaching, learning, research, and approved business activities of the University. You should always consider whether email is the appropriate method for a particular communication and whether the content of the email is in line with both this policy and the University’s wider policies. In general, you should not:

* send or forward chain mail, junk mail, cartoons, jokes, or gossip;
* create or transmit any offensive, obscene or indecent images, data, or other material (other than for reasons specified in 4.3 below);
* create or transmit material which is designed or likely to cause annoyance, inconvenience, or anxiety;
* create or transmit of material that is abusive or threatening to others, serves to harass or bully others, discriminates, or encourages discrimination on racial or ethnic grounds, or on grounds of gender, sexual orientation, marital status, disability, political or religious beliefs, or otherwise contravenes our policies;
* contribute to system congestion by sending trivial messages, copying, or forwarding emails to those who do not have a real need to receive them, or using “reply all” unnecessarily on an email with a large distribution list;
* sell or advertise using our communication systems, or broadcast messages about external business;
* promote career or business opportunities, unless this is directly relevant to your role e.g. as a member of the Careers team promoting opportunities to students, a department sharing relevant opportunities internally with your own students, or HR advertising internal job vacancies to staff;
* agree to terms, enter into contractual commitments, or make representations by email unless appropriate authority has been obtained;
* send emails from another person’s email address (unless authorised);
* create or transmit material which brings the University into disrepute;
* create or transmit of material that is illegal;
* transmit confidential material concerning the activities of the University to a third party, without the appropriate authority;
* transmit material that infringes the copyright of another person, including intellectual property rights;
* undertake activities that unreasonably waste staff effort or networked resources, or activities that unreasonably serve to deny service to other users;
* undertake activities that corrupt or destroy other users' data or disrupt the work of other users;
* create or transmit defamatory material or material that includes claims of a deceptive nature;
* undertake activities that violate the privacy of others or unfairly criticise, misrepresent others; this includes copying distribution to other individuals; or
* create or transmit anonymous messages or deliberately forge messages or email header information, (i.e. without clear identification of the sender).

4.2. The University permits the use of its IT facilities by students, staff, and other authorised users for a reasonable level of personal use. An absolute definition of reasonable is difficult to achieve but certainly includes (but is not necessarily limited to):

* a level of use that is not detrimental to the main purpose for which the facilities are provided;
* priority must be given to use of resources for the main purpose for which they are provided;
* not being of a commercial or profit-making nature, or for any other form of personal financial gain;
* not be of a nature that competes with the University in business;
* not relate to any use or application that conflicts with an employee's obligations to the University as their employer;
* not be against the University's rules, regulations, policies, and procedures and in particular this email policy;
* not to send, forward or read private emails at work which you would not want a third party to read.

4.3. It is recognised that, in the course of their work or research, individuals at the University may have a requirement to transmit or receive material that would normally be defined as offensive, obscene, indecent, or similar. In the case of properly supervised or lawful research purposes it is acceptable to do so. If in doubt advice should be sought by contacting your line manager in the first instance.

4.4. All communications should consider and uphold the duties required of the University, including (without limitation) the public sector equality duty, the applicable principles of safeguarding, the principles of the Prevent duty, and the University’s duty to uphold fundamental freedoms (including freedom of speech). Members of the University community should recognise and refer for review any communications that do not meet these requirements.

**5. Account management: storage, retention, and auto-deletion**

* 1. The appropriate management of email accounts is essential for compliance with legislation and reduces the risks associated with the unnecessary storage of information. A “one size fits all” approach to email retention is inappropriate in the University’s environment when it comes to management of emails. The named, exclusive user of a Microsoft Outlook email account, which they have been allocated, should ensure that they manage what is retained or deleted, based on the needs of their department and any legal requirements or regulations specific to their area of work. Account holders should review their practice regularly in line with the University retention schedules and any specific departmental requirements, to ensure they remain appropriate.
  2. Each account’s owner (including the named owner of resource email accounts) should ensure that they actively manage and ensure appropriate 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.
  3. Any emails saved in an individual’s mailbox are at risk of deletion if the named account holder leaves the University. Anyone leaving the University should consider how information they may have in that account should be transferred to other colleagues.
  4. All emails that need to be stored securely as a University record should be copied or saved into a case management system or network storage, as soon as reasonably possible, so that the records are easy to locate and can be retained within that system’s data retention policy. 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.
  5. Users should be familiar with any additional departmental policies that relate to the processes for securely storing important messages, and any additional processes for file organisation and naming conventions. When managing email accounts, care needs to be taken to ensure any emails containing University records are given an appropriate file name and location to facilitate ease of retrieval and deletion. In some circumstances it may be appropriate to save an attachment rather than the entire email.
  6. Individuals are responsible for managing the content of the network and cloud data facilities allocated to them. This includes shared folders they are responsible for. It is everyone's responsibility to periodically check the contents of these folders and consider whether to retain or delete each document, in line with their departmental record retention schedule. This is particularly important for emails that contain personal data and are therefore subject to Data Protection Legislation.
  7. Subject to the above paragraphs, if you have any emails in your inbox or other email folders that were received twelve or more months ago, you should decide whether to:
* delete the email;
* save either the entire email, or just a significant attachment, to a folder on the personal, University network drive allocated to you; or
* 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
* transfer the content, and record of the origin/sender/date of the email to a case management system or departmental database.

5.8. In reaching a decision as set out in paragraph 5.6 above, you should consider:

* compliance with University and department policies and guidelines, normal practice, and Data Protection Legislation;
* the likelihood that the email might be needed in the future and the potential consequences if that email is unavailable; and
* that you might need to search for that email and release it outside of the University because of a Freedom of Information Act or Data Protection Subject Access request.

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

5.10. When you delete an email from the inbox this is not actually “deleted,” it is moved into the Deleted Items folder, where it will remain until it is either deleted by system rules or permanently deleted by the account holder.

5.11. **Any items older than 12 months in the Deleted Items folder 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.

5.12. **Sent Items of each email account older than 24 months are automatically deleted.** It is, therefore, essential that any significant email conversations or attachments are saved in an appropriate location without delay to ensure these are accessible when required.

5.13. **Any emails left in the Inbox folder are automatically deleted after 24 months.** It is, therefore, important to ensure that any subfolders in the mailbox are not branched from the Inbox. For more information on this please consult the [IT Help Pages](https://help.chi.ac.uk/outlook-managing-your-emails).

5.14. In some areas of work, particularly those handling extremely sensitive personal information, it may be appropriate to have an additional policy of more frequent deletion of items from email folders and calendar appointments than the standard deletion periods outlined above. For further information on how to permanently delete emails please consult the [IT Help Pages](https://help.chi.ac.uk/outlook-managing-your-emails).

**6. Mailbox security**

To minimise the risks of cybercrime and information security posed by email, and to effectively manage your mailboxes, you should:

6.1. Lock your screen by pressing the Win + L key (Win is the windows key) at the same time on your keyboard any time you are any from your desk, even if you are away for a moment.

6.2. Never forward University emails to your home email address.

6.3. Where possible, send hyperlinks to documents rather than attachments. This contains the information a unique location rather than in several users’ mailboxes and/or sent items.

6.4. Avoid using email sub-folders within your mailbox as long-term storage 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 cloud or network location e.g. a restricted shared folder and give them an appropriate file name.

6.5. Carefully check the auto-complete email addresses 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”. You may find it helpful to switch off this facility altogether, which is explained on the [IT Help Pages](https://help.chi.ac.uk/turn-auto-complete-outlook).

6.6. 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.

6.7. Use the University’s standard email signature, containing your contact details, for both external and internal email. There is guidance on this [here](https://help.chi.ac.uk/setting-your-staff-signature-your-university-email).

6.8. Unless completely sure of the source, do not download or install anything received in an email from external sources without consulting IT Services.

6.9. Be careful opening unsolicited emails from unknown sources or an email which appears suspicious. Inform IT Services immediately if you do open an email that seems suspicious.

6.10. Be vigilant if you access your email outside of the workplace, such as on your phone.

**7. Instant Messaging**

7.1. Every University email account holder also has access to instant messaging services such as the chat function in Microsoft Teams. The purpose of instant messaging services is to facilitate day-to-day business activity. The contents of the messages are University records and subject to disclosure under Data Protection legislation and the Freedom of Information Act 2000 in the same way emails are. Individuals are responsible for managing their instant messages and are advised to periodically check the contents and consider whether to retain or delete each message. This is particularly important for communications that contain personal data and are therefore subject to Data Protection legislation.

7.2. **The University’s retention policy in place for Teams is to delete messages after 12 months.** This applies to one-to-one and group conversations (Chats), Teams Channels and Teams Meetings.

**8. Calendar sharing and delegate access**

8.1. Every University email account holder has access to a Microsoft Outlook calendar, which is used to arrange a mutually convenient appointment with one or more staff, students, and external contacts. Options within Outlook allow you to manage the level of information about your appointments that colleagues can see in your calendar, for example free/busy information only or full access. You should be careful not to share calendar information more widely than necessary.

8.2. By default you should only publish ‘free/busy’ calendar information, for the purpose of keeping colleagues updated. You may want to give permission to view the detail of appointments to specific individuals, and/or members of your immediate team or department. In this case, remember that they can also see the content of any attachments to calendar appointments. For information on how to review the privacy settings of your calendar please visit the [IT help pages](https://help.chi.ac.uk/sharing-your-calendar).

8.3. You should consider who has access to the full details of your calendar before recording any personal data, commercially sensitive, or otherwise private information in an appointment. In these cases, you should tick the box to mark the appointment ‘Private’, which will mean that no one else can see the details.

8.4. **Calendar appointments older than 24 months are automatically deleted**. It is, therefore, essential that any appointments or attachments required for reference after this period are saved in an appropriate location to ensure these are accessible when required.

**9. Email etiquette**

9.1. Emails are not contextualised by body language, facial expressions, or tone of voice. This can lead to miscommunication. By thinking carefully about the contents of our emails, and practicing good email etiquette, we can maintain an efficient, collaborative, and positive working environment.

9.2. The following are generally accepted email etiquette which we encourage you to bear in mind before sending any email:

* Include a relevant subject line that does not include the names of individuals.
* Try to avoid using acronyms or jargon, unless you are sure that they will be understood.
* Keep your messages short, clear and to the point.
* Avoid sending personal remarks.
* Do not send or respond to emails when you are feeling angry, as you may regret it later.
* 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.
* When forwarding emails, tell your correspondent who you have forwarded a message on to, so they know who will reply. Take care to review the information at the bottom of the email chain before forwarding on to ensure personal data is not shared more widely than necessary.
* Use the “To” field for intended recipients of an email and those required to take action, the “CC” field if you are adding a recipient for information only, and the “BCC” field if recipients do not need to know who else has received the message. Using BCC is especially important when emailing large groups to avoid the risk of someone accidentally clicking “Reply all”.
* 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 may be set to “Reply all”, but it is very easy to [change the default setting to “Reply”](http://help.chi.ac.uk/changing-default-reply-setting-office-365) – click for guidance on the [IT Help pages.](https://help.chi.ac.uk/changing-default-reply-setting-office-365)
* Use the “High Importance” flag if relevant, but do not overuse this or it loses its impact.
* 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](mailto:help@chi.ac.uk).
* Avoid typing using all CAPITALS for text as this may be considered to be SHOUTING.

**10. Further information**

For the most recent guidance and policies relating to privacy and Data Protection, including advice on determining a compliant departmental [retention policy,](https://staffnet.chi.ac.uk/data-protection/content/guidance-and-policy) please visit the pages on the intranet <https://staffnet.chi.ac.uk/data-protection/content/guidance-and-policy>. Please also refer to the links identified in section 2 of this policy. You may also find the University’s high level Records Retention Schedule a helpful guide to inform your retention policy.