IT Acceptable Use Policy
Email and Collaboration Tools Procedure

Effective Date: 22/09/2022
Supersedes: May 2019 (Email Procedure)
Last Review: 06/01/2024
Next Review: 31/01/2025

I. Scope

1.1 These procedures apply to all users in the King's community – Staff, Students, Affiliates, Researchers, and contractors. In accordance with the IT Acceptable Use Policy.

1.2 These procedures cover the use of KCL provided email accounts assigned to individuals or groups, and instant messaging via university provided means including (but not restricted to) Microsoft Teams, Yammer and Zendesk. It also applies to other electronic software based collaborative tools that may be used by the university.

1.3 Emails and instant messages sent, received or generated in the course of all university business, academic and administrative, are the property of the university. The university owns the intellectual property rights in all emails and instant messages generated by its staff in the course of the university's business. Emails and instant messages sent using university provided systems are searchable under SAR legislation, and for official university procedures such as disciplinary action or legal proceedings.

2. Important Dos and Don'ts

2.1 Auto-forward is not enabled on university email accounts and users must not redirect or forward emails in their university account to an external email account (e.g. Hotmail or Gmail) as such accounts may store data outside the EU and they may be in breach of data protection legislation.

2.2 Users should always double-check that they have the correct contact before sending emails or messages. Be aware that the auto-complete address list can become corrupt and result in the email or message being sent to someone unexpected. If emails or messages are sent to an incorrect person containing confidential or sensitive personal data, users must fill in a data breach form as per the Data Breach Management Procedure.

2.3 Never put personal or confidential data in the body of an email, message or in an attachment, unless the email, message and/or the attachment is encrypted. NOTE: payment card data must never be emailed, whether encrypted or not. Select the link for more guidance about Data Loss Prevention.

2.4 When sending confidential information, alert the recipient so that they only open the document in a secure environment. If you are unsure of the confidentiality of the data you are sending, please refer to the Information Classification Procedure.

2.5 We do not allow the integration of third party add-ons, services or software to the KCL email platform that are not offered by KCL. By allowing integration the third party must be given access to our systems and network, and often requires the circumventing of our security which is in breach of the IT Acceptable Use Policy. If you feel that you have a business need to integrate a third party add on, software, or service to your King's email please contact itassurance@kcl.ac.uk for a discussion on a case-by-case basis.

3. Etiquette

3.1 Use the correct contact method for the purpose. Emails may be more formal and Instant messaging functions are informal, but polite and courteous language should always be used when contacting others.

3.2 Be mindful of "spamming" colleagues with multiple messages and emails. Where possible include your full initial message with your first contact.

3.3 Consideration should be taken with the use of GIFs, images and emojis to avoid offence or upset to others.

3.4 Respect a person's online status. If your recipient is shown as offline, in a meeting, do not disturb, or out of office, sending an email instead may be more productive and better appreciated.

4. Email - Out of Office

4.1 To maintain the high service standards of the university and to ensure continuity of the university's business, users who are going to be unable to access their emails for whatever reason (e.g. whilst on leave) must make appropriate arrangements to ensure that their emails are properly dealt with in their absence. There are various solutions available including:

- Auto-forwarding emails to other **King's** accounts, where both parties are in agreement.
- Out-of-office message that provides alternative contact details as appropriate.
- Enabling delegated access on a read-only or read/write basis.

4.2 Users who work part-time should:

- Activate the out of office assistant on non-working days/hours; or
- Alter the email signature to stipulate the work pattern so people know what days and times you will be available to contact.

4.3 In exceptional circumstances, with the authorisation of either the department head or Human Resources, IT may remotely set an Out of Office message on an account. Some examples of situations in which this may be requested include:

- Illness or incapacitation such that the individual cannot access their account remotely
- Prolonged absence from the workplace
- Suspension

5. Email - Delegate Access/Shared Folders

5.1 Users must never share their university email account password.

5.2 Teams and colleagues should establish how to best work collaboratively to ensure that data is shared securely. Some options include:

- Establishing shared email folders
- Using Microsoft Teams or a SharePoint site
- Requesting a shared mailbox

5.3 Where mailbox access is required, delegate permissions should be granted from the owner of the mailbox.

6. Leavers

6.1 Email addresses and collaboration tool accounts are deactivated and deleted when a user's formal association with the university ends.

6.2 As part of the leaving process, departing staff must forward on any emails or calendar appointments to remaining colleagues and ensure any personal content is removed from their mailbox on leaving the university. This is because all mailbox content will be inaccessible to the individual from the date of the account being disabled.

7. Encryption

7.1 Encryption is the method by which plain text or any other type of data is converted from a readable form to an encoded version that can only be decoded by another entity if they have access to a decryption key. Encryption is one of the most important methods for providing data security, especially for end-to-end protection of data transmitted across networks.

7.2 Use the university-provided encryption methods for highly sensitive content. This includes emails sent within and outside the King's network.

7.3 Select the link for more information about encryption and data loss prevention.

8. Anti-Virus

8.1 Users should be wary about opening attachments from unknown sources and always virus check suspicious or unexpected attachments. To do this, save the document to a chosen folder. Once saved, right click the document and select **Scan with OfficeScan**.

8.2 Report any unusual activity to IT Service Desk. Select the link for more information about IT Security.

8.3 Users should refer to the Code of Connection regarding the use of antivirus.

9. Email - Spam and Phishing

9.1 Spam can be defined as "the mass electronic distribution of unsolicited email to individual email accounts". Junk mail is usually a result of spamming. Spam and junk mail are regarded as interlinked problems. A certain amount of junk mail is blocked at the mail gateways.

9.2 Users should note that the university's anti-spam facilities may result in messages going "missing", as the university will take steps to prohibit spam and all-staff emails (and **Reply All** storms).

9.3 Phishing is targeted spam looking to impersonate and exploit known business relationships (e.g. a trusted source that a user might expect to hear from as part of their day to day work, such as IT Service Desk).

9.4 Be wary about opening attachments from unknown sources and always virus check attachments. To do this, save the document to a chosen folder. Once saved, right click the document and select **Scan with OfficeScan**.

9.5 Select this link for more information about phishing, what to look out for and how to report a suspected incident.

10. Email - Setting Restrictions

10.1 From the toolbar, selecting **Options** > **Encrypt** while composing a message allows a user to set up restrictions for the individual email, including simple encryption. Other options are:

- Selecting **Do Not Forward** prevents people from forwarding, copying or printing the email.
- Selecting **King's College London** – **Confidential** means the email content can be modified but cannot be copied or printed.
- Selecting **King's College London** – **Confidential View Only** means the content cannot be modified.

10.2 Select the link for more guidance about Data Loss Prevention.

11. Quotas and Limits

11.1 Every user has a designated email quota. A warning message will be sent when the mailbox reaches near capacity. The final email that takes a user over their limit will always be delivered. Once over the quota, no further email can be delivered to the mailbox until the mailbox is below the limit. Remember that emails are stored in **Recover Deleted Items** folder and this will also need to be emptied. For more information select Recover Deleted Items.

11.2 An email greater than 15MB cannot be guaranteed to be accepted for delivery to a King's account or to be accepted for transmission by the email servers.

11.3 The university reserves the right to fix and adjust the maximum size allowed for any single message and attachments within the university email and collaboration tools systems.

12. Public and Private Mailing Lists

12.1 All users of the university's email service are automatically added to a series of university circulation lists. These public lists enable the university to disseminate important information to targeted user groups in an efficient way. The lists are actively moderated, and all prospective messages should be submitted for approval before they are released for circulation. Some lists have authorised users who can bypass this moderation, such as the moderators themselves.

12.2 Moderation is undertaken by designated gatekeepers in accordance with published university guidance here: Mailing Lists at King's.

12.3 University interest groups and administrative units may, for their own convenience, set up private lists. Although these lists are hosted centrally, moderation and maintenance duties are the sole responsibility of list owners.

13. Good Housekeeping

13.1 Use meaningful subject lines to ensure emails can be readily searched, located and retrieved.

13.2 Check email and messaging tools regularly, deleting unwanted messages immediately. Delete those messages that are no longer valid, relevant or useful.

13.3 Clear out the mailbox regularly, filing and archiving logically, as this will prevent the mailbox getting full and allow easier retrieval of relevant emails when requested. Note: mailboxes at King's by standard have a quota of 49.5GB however this is subject to change as per the **Exchange Online Limits**.

13.4 Use an email signature, detailing full contact details and address as standard. Advice on what should be included should be sought from your line manager.

13.5 Do not print out emails unless absolutely necessary.

13.6 Information should not be stored on email indefinitely. If there is a requirement to store an email for an extended amount of time, users should transfer it to another more appropriate storage solution such as OneDrive for business or Sharepoint. PST files should not be used.

14. Accessing another user's account

14.1 IT will never automatically give a user access to another user's mailbox as there may be personal data contained within the email account that others do not have a right to access and view.

14.2 Notwithstanding, there may be circumstances in which it is necessary to access certain emails within an individual's account without their consent or knowledge, including but not limited to:

- Where there is a compelling business need (for example, to comply with a Subject Access Request or a Freedom of Information request)
- Death of a colleague
- Prolonged absence
- Suspension or dismissal
- Investigation into employee or student performance and behaviour
- Compliance with lawful requests for information from government and law enforcement agencies.

All requests must be via itassurance@kcl.ac.uk to be considered, each request should provide a business case, attached permission from the head of department, and confirmation that all other alternatives have been explored (i.e. contacting the individual concerned).

14.3 The requestor will not automatically be given access to all emails within the account to ensure the privacy of the individual is protected. Requests should include a list of key words

and a date range for the search. Such lists should be comprehensive to permit search across all parts of the emails (To, From, Subject, Date, Body).

14.4 Results of any search will be stored in a Discovery mailbox and the emails reviewed by a member of IT Assurance to check for any personal data. Access to the Discovery mailbox will be limited to nominated individuals and limited to a maximum of five days. There will be no extension to this time limit. The start date for access is to be agreed between IT Assurance and the investigator.

14.5 An investigator may print or save pertinent emails but must keep a detailed record of any so kept. Further, an investigator must keep secure any personal data obtained and permanently delete it when it is no longer needed.

14.6 The individual whose account has been accessed without their consent and/or knowledge must be informed of that access as soon as practicable.

14.7 Where the staff member has left the university and access to their emails is required, deprovisioning of the account will be put on hold.

Appendix A-change log

Version	Date	Name	Role	Changes made
V1.2	21/04/23	Lauren Middlemist	IT Assurance Apprentice	Change control log added as Appendix A.
V1.3	07/09/2023	Kirsty Lynch	Senior IT Assurance Officer	Addition of section 2.5