Kingston University

Acceptable Use Policy - Email

Effective from 20th June 2023
Next review due May 2024
Version 2.0

Contents

1 Equality Statement

Because we value diversity and equality highly we have designed this policy to be fair and inclusive. In putting this policy into practice we expect all members of the University community to abide by the spirit and detail of the Equality Act 2010 and the Town House strategy for equality, diversity and inclusion

2 Policy Title

Acceptable Use Policy – Email

3 Policy Statement

Kingston University provides an email system for staff and students in order for them to efficiently carry out their work and study duties. When using the KU email system individuals should be aware that they are representing the University and so should do so responsibly.

This policy provides guidelines on using the KU email system effectively and securely.

4 Policy Scope

This policy applies to all users of the KU Email system. Email is available to all users within the KU community who have agreed to abide by the Acceptable Use Policy for IT facilities.

5 Governance & Review

The policy owner will review the policy content annually at least.

The policy owner will review the policy immediately in circumstance where any detail within the policy has significantly changed.

This policy will be signed in the first instance by the policy owner, with subsequent approval by the CIO.

All University policy documents must be signed and submitted to the University Secretary's office for record.

6 Related Resources

Policies and regulations for Kingston University

7 Policy:

Please note that at time of publication the University email system is provided by Microsoft through their Office 365 product. Users of the KU email system are bound by the terms and conditions of this service.

7.1 Responsible Use of Email

Users sending emails from any KU owned domain (e.g. xxxxxx@kingston.ac.uk or xxxxx@kcg.co.uk), are seen as representatives of KU and as such should act in a responsible manner:

- The sending of abusive, offensive, defamatory, racial or sexual content within an email is strictly prohibited.
- The sending of emails with content in breach of the University's 'Prevent' duty to safeguard staff and students from radicalisation is strictly prohibited.
- The sending of emails that could be considered libellous to an individual or organisation is strictly prohibited.

7.2 Personal Use of Email

Users are strictly prohibited from using the KU email system for personal use, and personal email should not be used for work purposes. The KU email system is intended solely for official and academic purposes related to the university. Personal use of the email system, such as sending non-academic or non-official communications, is strictly against the university's policies.

7.3 Email Security

Email is not a secure form of communication and as such users must realise that any information sent via email may be seen by others. Users are responsible for ensuring they don't compromise information security:

- The security of email content cannot be assured. It is important that information of a personal, financial or sensitive nature is not communicated by email, and an alternative, secure form of communication is used instead.
- Users must not intercept or access other users' email without proper grounds and authorisation, and in accordance with the law.
- Users are strictly prohibited from automatically forwarding incoming messages from their university accounts to an external email account unless they are exempt for business-critical reasons or have obtained explicit approval from Vice-Chancellor/Director of Human Resources (or equivalent)/Chief Information Officer (staff/affiliates) or the Executive Director of Student Services/Chief Information Officer (students).

7.4 Monitoring and Access to Email

The University may at any time permit the inspection, monitoring, or disclosure of email content;

7.4.1 When required by and consistent in law.

The University does not automatically comply with all requests for disclosure, but evaluates all such requests against the precise provisions of the Freedom of Information Act, Data Protection Act, The Regulation of Investigatory Powers Act, and other laws concerning disclosure and privacy, or other applicable law.

7.4.2 Policy compliance.

At the written request of the Vice-Chancellor/Director of Human Resources (or equivalent)/Chief Information Officer (staff/affiliates) or the Executive Director of Student Services/Chief Information Officer (students) if there are reasonable grounds to believe that violations of University policies have taken place.

7.4.3 Access to the university account is terminated on the day users officially leave the university. However, the mailboxes of these users are retained for an additional 90-day period from the day they leave the university and deleted to adhere to data retention policies and maintain data security and privacy.

7.4.4 It is not standard practice for IT Services to grant access to the mailbox of a deceased

staff member, student, or those who have left the University.

However, in certain critical business situations where accessing the mailbox is necessary, it is highly recommended to first obtain consent from former members of staff or students. If obtaining consent is NOT feasible, the request must be approved by the Vice-Chancellor/Director of Human Resources (or equivalent)/Chief Information Officer (staff/affiliates) or the Executive Director of Student Services/Chief Information Officer (students).

7.4.5 The University reserves the right to monitor email in order to;

- carry out system management, problem resolution, maintenance and capacity planning, to correct addressing problems or for similar reasons related to performance or availability of the system.
- to address security issues, including virus management and authorised surveillance, including tracking unauthorised access to a system.
- to meet time-dependent, critical business or operational needs or to carry out records management responsibilities; e.g. to conduct business during a crisis if

an employee is absent. The user will generally be informed at the earliest opportunity if this form of access is necessary.

7.5 SPAM

SPAM is defined as bulk email communications that are unsolicited, for example; an invitation to a personal birthday party sent to the entire KU user community would be considered SPAM:

- Users should not send SPAM email to other University staff or students.
- Users should not send SPAM email to non-University individuals.

7.6 Attachments

Users should avoid sending personal data and sensitive information such as financial data via an attachment.

Users must not send harmful or dangerous content as email attachments such as virus or worms.

The sending and forwarding of chain emails is also prohibited.

The sending of multimedia content such as video or music files must be considered carefully, as this can have a serious impact on network bandwidth. Where possible save such multimedia content to a shared area and send recipients a link to that area.

The sending of some attachments is blocked on the Email system; these include Executable files, JavaScript files and security certificate files. A full list is available from Information & Technology Services.

7.7 Infringement

Anybody using Kingston University IT facilities agrees to abide by the terms of any applicable policies. Users who are found to have breached the terms of relevant policies may be subject to warnings, verbal and written. In serious cases individuals will be subject to the University's disciplinary procedures.