Kingston University

Acceptable Use Policy – IT Facilities

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 – IT Facilities

3   Policy Statement

It is a condition of use of the University's IT facilities that all staff, students and other authorised individuals agree to abide by the terms set out in this acceptable use policy.

Individuals agree to the terms of this policy when they sign their contract of employment or student contract.

4   Policy Scope

All users of Kingston University IT facilities, including any desktop computer, laptop, mobile device or other form of access to IT services. The policy includes all software services hosted by or managed by either IT Services or any faculty or directorate.

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:

7.1   Authorisation

Use of the University's IT facilities is restricted to staff, students and any other affiliates with the appropriate approval.

Only those with a University created user account may use the University's IT facilities, and must be authenticated using their own credentials.

7.2 Access

Access to IT facilities on any of the University's campuses is available during published opening hours.

Remote access to University IT facilities via My Desktop Anywhere or Virtual Private Network if appropriate, is available at any time unless otherwise publicised, although it should be noted that in the event of a technical issue, IT support is generally only available during weekdays from 08:00 to 18:30.

7.3 Conditions of use for Hardware and Software

Users must not in any way cause any form of damage to the University's computing equipment or software, nor to any of the rooms and their facilities and services which contain that equipment or software, nor to any of the network wiring infrastructure or communications equipment. The term "damage" includes modifications to hardware, software or infrastructure which, whether or not causing harm to the hardware or software, incur time and/or cost in restoring the system to its original state. All costs associated with repairing or replacing damaged equipment or software and/or in providing temporary replacements will be charged to the person or persons causing the damage. The costs will be determined by the University.

Users must periodically review and update their regulatory training to remain compliant according to relevant legal and regulatory requirements.

Users of IT facilities must be aware of their cyber security and data protection responsibilities by having completed the relevant compliance courses provided by the University, including periodic refresher courses.

Users must not modify any software, nor incorporate parts of any software into their own work, without written permission. If in doubt contact the Service Desk.

Users must comply with any instructions or regulations displayed in and around computing facilities.

Users must not introduce any virus, worm, malware, trojan horse or any other "nuisance" program or file onto any system or take any action to circumvent or modify any precautions taken by the University to prevent "infection" of its machines.

Users must not use IT facilities for sending any message, textual or graphic or voice or video, that is offensive, abusive, obscene, defamatory, racist or otherwise unlawful. Users must not initiate or spread electronic chain mail. Any electronic mail must be relevant to the user's course of study or job within the University and it must be sent only to those users to whom it is relevant.

Users may only access their own files and files which they have been given express permission to access.

Users must not use another individual's username nor permit or allow another user to use their own username.

Users must not allow any password associated with their username to become known to another user. The user may be held responsible for any unlawful action carried out under their computer account .

Users must not make known any other passwords which may be supplied to them in order to enable access to subscribed electronic resources.

Users must not connect any equipment to the University wired network without prior approval from the Cyber Security Manager.

Every user of network facilities shall comply with any rules published for use of the networks and/or any IT systems to which they have access over those networks.

Interference with or removal of printout which belongs to another person is not permitted. Uncollected printouts will be disposed of.

Printing credit in a student account will not be refunded at any time during the year or at the

end of the academic year. Continuing students will carry their printing credit to the following year. Students leaving the University will not be refunded.

7.4   Behaviour

The creation, display, production, downloading, uploading and circulation of offensive material in any form or on any medium is forbidden.

Users must respect the rights of others and should conduct themselves in a quiet and orderly manner when using facilities.

No equipment should be moved from its designated place or be tampered with in any way.

Avoid eating or drinking in close proximity to IT facilities.

7.5   Private and Commercial Use

The use of any of the University's IT facilities for commercial gain, as well as for private work unconnected with a course or job role, or for work on behalf of others, is not allowed unless with prior approval from a member of SMT.

7.6   Use of Janet and the Internet

Use must comply with the Janet Acceptable Use Policy (available from https://community.jisc.ac.uk/library/acceptable-use-policy),The Janet Network ("Janet") is the communications network operated by Jisc Services Ltd (Jisc) to serve UK education, research and other public sector purposes.

Janet may be used for any legal activity that is in furtherance of the aims and policies of Kingston University. Where Janet is being used to access another network, any abuse of the acceptable use policy of that network will be regarded as unacceptable use of Janet.

7.7   University Rules for using Janet and the Internet

The Janet Acceptable Use Policy applies also to the internal University network.

7.7.1   Commercial use is prohibited. Commercial use refers to any activity connected or involving any trade, profession, vocation or business not being any part of any function or purpose of Kingston University whether carried on solely or jointly or severally and/or whether or not with a view to profit or benefit any person or personal body other than Kingston University.

7.7.2   Recreational student use is allowed but students have to release the workstations if needed for course-related work. Unreasonable or recreational use by staff is prohibited during working hours.

7.7.3   Anonymous Email or any type of anonymous electronic information must not be sent.

7.7.4   Offensive material must not be sought or knowingly received.

7.7.5   Network services (e.g. Ftp or Web servers) must not be set up without first being registered with IT Services. The person setting up the service will be held responsible for the secure operation of that service.

7.7.6   The University's Information Security Policies should be read as part of the University's regulations.

7.8   Disclaimers

In order to comply with the requirements of the Data Protection Act 2018, once a student

leaves the University having completed their course the University will not retain any information created by the student, including emails, files or other content for longer than it is needed. Students wishing to retain access to data they have produced should make their own arrangements to copy that data elsewhere. The University will not be held responsible for student data that is not retained.

Staff accounts are disabled upon contract termination. The University will not be liable for non-retention of staff data beyond this time.

7.9 Monitoring & Access to IT Systems & User Accounts

The University may at any time permit the inspection, monitoring, or disclosure of IT Systems and Data;

7.9.1　When required by and consistent with English law. The University 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.

7.9.2　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. Existing policies can be found at http://www.kingston.ac.uk/aboutkingstonuniversity/howtheuniversityworks/policiesand regulations/

The University reserves the right to monitor IT Systems:

7.9.3   For instance to carry out system management, problem resolution, maintenance and capacity planning, to correct problems or for similar reasons related to performance or availability of the system.

7.9.4   To address security issues, including virus management and authorised surveillance, including tracking unauthorised access to a system.

7.9.5   The University may access, with written authorisation 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) , the content of user accounts.

7.9.6   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 when information is required, or prolonged absence of an employee when information in the User's account is required. The User will generally be informed at the earliest opportunity if this form of access is necessary.

7.10 Copyright Protection

The Copyright, Designs and Patents Act,1988 (including its subsequent amendments and Statutory Instruments) applies to all users of the University's computers. Users must take care not to infringe copyright during the course of their work or study. The University subscribes to a number of licences enabling use of specific materials including some digital copying. Information on how to avoid infringing copyright may be found on StaffSpace and My Kingston.

7.11 Disciplinary Procedures

Failure to comply with these conditions of use for facilities may result in the following procedures being invoked:

7.11.1   Withdrawal (whether permanent or temporary) of access to University IT facilities. Such withdrawal may be invoked immediately after suspected breach of IT regulations has occurred. Reinstatement of access to IT facilities will be through normal disciplinary procedures.

7.11.2   Recommendation to proceed through the University's disciplinary processes.

7.11.3   Referral to the Police for possible prosecution. Where appropriate.

THE DATA PROTECTION ACT (2018) applies to all users of the University's computers who process personal data (information relating to a living person). Further information and guidance regarding the requirements of the Act may be obtained from the University's Data Protection Officer, based in the University Secretary's Department, or from the website of the Information Commissioner's Office: http://www.ico.gov.uk