Computer Resources - Acceptable Use Policy

Version	Date	Changes	Author
1.0	2017	New Policy	Chris Linton (Cyber Security Manager)
1.1	November 2023	abuse@qub.ac.uk added as primary contact. Updated staff/student social media policy links.	James Vincent (Cyber Security Manager)

Overview and Scope

The purpose of this policy is to make all users aware of their duty to use the University's computer resources responsibly, professionally, ethically, and lawfully and with due respect for others. For the purposes of this policy the term "computer resources" refers to any University IT infrastructure or service made available to you, including networks (wired or wireless), PCs and other devices, software, and services such as file storage, email and Internet access. Students and staff who connect their own IT devices to the University's network or use their own devices to access University services (e.g. from home) are particularly reminded that such use also requires compliance with this policy.

All users must adhere to this policy. Users in breach of this policy will be liable to disciplinary action under University procedures.

If you are unsure whether any of your computing activity may breach University policies, you should seek advice before proceeding. You can contact Digital & Information Services for advice by emailing cybersecurity@qub.ac.uk.

Users should read this policy in conjunction with the Student Computing at Queen's Acceptable Use Guide and Staff Computing at Queen's Acceptable Use Guide, as appropriate available at http://go.qub.ac.uk/itpolicies . These outline your key responsibilities and give examples to illustrate this policy.

Summary

University computer resources are provided for bona fide University activities. The use of these resources must be legal, honest, and respectful of others. This includes:

1. Complying with all relevant laws and regulations regarding computer and data use
2. Being considerate to others
3. Using resources responsibly: irresponsible use includes collection, creation, display, and circulation of material that others may reasonably find offensive.

Legal Compliance

Users must always comply with relevant legislation. The range of legislation is potentially very wide but users should be particularly aware of the Computer Misuse Act; the Regulation of Investigatory Powers Act: the Telecommunication Regulations Act, and legislation relating to the protection of children, to human rights and obscene publications.

Users must not knowingly access data that they are not authorised to access.

Users must not deliberately create, retain, send, access, or display unlawful material.

Users must not create or transmit defamatory material.

Users must respect the copyright of all material made available by the University and third parties and not use, download, copy, store, or supply copyright materials including software and retrieved data other than with the permission of the copyright holder or under the terms of the licence held by the University.

Consideration for Others

Users must not deliberately create, retain, send, access, or display any material which, if viewed by others, could reasonably be construed as likely to cause offence or distress, regardless of whether such material is legal. The only exception to this is material used for properly authorised and lawful academic purposes.

Users must respect the dignity and privacy of others and must always consider how their online behaviour may affect others.

Identifying Yourself Online

Users must identify themselves honestly and accurately when communicating online. Users must not share their password or Smart Card with others, or use another's password or Smart Card.

Users must not attempt to gain unauthorised access to any facility or service within or outside the University.

Use of Resources

Users must follow the security advice from Information Services in relation to protecting their computer from ransomware, ‘phishing’ emails, viruses, and malware. The advice is found on the Queen's website at this address - http://www.qub.ac.uk/directorates/InformationServices/Services/Security/.

Users must take all reasonable care not to introduce any computer virus or other harmful or nuisance program or file onto any University computer resource; and must not take any deliberate action to circumvent any University protective security measures e.g., virus control or device management.

Users must not waste resources. While reasonable personal use of University computer resources is permitted in some circumstances, personal use must not unreasonably impact on the resources available to the University and to other users.

Bring Your Own Device (BYOD)

Users connecting their own devices to the University network, or using their own devices to access University systems such as email, must adhere to this policy during all such use.

If you use your own device to access or store University data then you must fully comply with the University's Data Protection Policy and Information Security Policy http://go.qub.ac.uk/itpolicies in order to protect that data.

Social Media

Users must adhere to this policy when using University computer resources to access social media sites (e.g. Facebook, Twitter). In addition, the University has implemented specific Social Media Policies for Students and Staff and users must fully comply with these.

Social Media Policy for Staff: https://www.qub.ac.uk/home/social-media/Filestore/Filetoupload,781846,en.pdf

Social Media Policy for Students: https://www.qub.ac.uk/home/social-media/Filestore/Filetoupload,781847,en.pdf

Monitoring

The University carries out routine logging and monitoring of its computer systems, including Internet and email traffic, and reserves the right to use such information in the event of any disciplinary or legal investigation. IT equipment and system logs may be subject to more detailed examination to assist in any disciplinary or legal investigation. The University reserves the right to act on any information obtained from online sources, including social media, if it indicates that a user is in breach of University policies or the law.

Users should be aware that their email and file store may be accessed by authorised individuals during periods of absence, for business continuity reasons.

Related Policies

Users of computer resources must fully comply with relevant University regulations and policies (http://go.qub.ac.uk/itpolicies), including:

1. The Conduct Regulations for students
2. The Code of Conduct for staff
3. The Information Security Policy
4. The Data Protection Policy

Reporting

You can report any breach of the Acceptable Use of Computer Resources Policy to the IT Service Desk (02890 973760)/itservicedesk@qub.ac.uk or by emailing abuse@qub.ac.uk.

Staff may contact their line manager as appropriate.