



QUEEN'S
UNIVERSITY
BELFAST

DIGITAL &
INFORMATION
SERVICES

A photograph of a young woman with blonde hair, wearing a blue button-down shirt, smiling warmly at the camera. She is leaning over a desk, looking at a laptop screen. The background is softly blurred.

STAFF COMPUTING AT QUEEN'S ACCEPTABLE USE GUIDE

www.qub.ac.uk/is

INTRODUCTION

Version Control

Version No.	Author	Purpose/Change	Date
1.0	Chris Linton - Data Security Manager	Published version	17/09/2018
1.1	James Vincent – Cyber Security Manager	Updated personal use clause. Updated BYOD Updated contact email.	31/07/2023

INTRODUCTION

The use of Information Technology (IT) is an indispensable part of work for most staff at Queen's. To ensure that the full potential of IT is realised, it is important that you understand your responsibilities in relation to the use of University computing and online resources.

The purpose of this guide is to inform you about your responsibilities and to illustrate some of the issues addressed in the University's Computer Resources - Acceptable Use Policy. This guide should be read in conjunction with the Policy which you can download from the website at: <http://go.qub.ac.uk/itpolicies>.

UNLAWFUL ACTIVITY

As well as being a breach of the University's Computer Resources - Acceptable Use Policy, certain activities may constitute an offence in law. In particular, you should familiarise yourself with legislation relating to the protection of children, to human rights and to obscene publications.

If you are uncertain whether your computing activities may break any law, you should seek guidance by emailing infosec@qub.ac.uk before proceeding.



DATA PROTECTION REGULATIONS

If you are required to collect, process or use personal information (such as information relating to an individual who can be identified) on behalf of the University, you must adhere to the University's Data Protection Policy. For further information, contact the Information Compliance Unit in the Registrar's Office.

ACCEPTABLE USE

The purpose of the Computer Resources - Acceptable Use 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.

The policy states that you must not deliberately create, retain, send, access or display any material which could reasonably be construed as likely to cause offence to others.



The decision on whether or not an activity is "likely to cause offence" will depend very much on context and will be subject to grounds of reasonableness, but in essence you should avoid any activity which undermines the dignity of others and should always consider how your behaviour may affect others. In particular, you should not create, store, transmit or display the following material, in any format or under any circumstances:

- Sexually explicit or offensive material
- Material that is abusive or threatening or could be seen as harassing
- Material that expresses or supports sexist, racist, sectarian or homophobic views
- Material that expresses support for illegal activities or organisations
- Material that is designed or likely to cause needless anxiety to others
- Material that is defamatory, inflammatory or discriminatory

The policy is not designed to restrict academic freedom and a general exception is made for properly authorised and lawful academic purposes. If you are uncertain whether any use of your computer may cause offence to others, you should seek advice by emailing infosec@qub.ac.uk before proceeding. You should also be aware of your obligations as set out in the University's Code of Conduct (<http://go.qub.ac.uk/CodeofConduct>)

MONITORING OF ACTIVITY



The University reserves the right, consistent with relevant legislation, to exercise control over computer resources and to monitor their use to ensure efficient operation, to detect misuse and to supply evidence, if required, for use in disciplinary or legal proceedings.

Users should note the following:

- Traffic through email gateways is logged, including the source and destination, but not the content of email messages
- Internet and other network traffic through the caches and firewalls is logged, including sites visited, which can be traced back to individual computers

These logs are reviewed from time to time by authorised Digital & Information Services staff in order to monitor the efficiency of services. In the event of any disciplinary or legal investigation, Digital & Information Services may be asked (by the University or other authority) to assist in the collation of information, including information from logs, for more detailed examination. The University reserves the right to act on any information obtained from these logs or other sources if it indicates that a member of staff is in breach of the Code of Conduct for staff or other University policies.

In reviewing or investigating Internet activity in particular, the University recognises the possibility that sites may have been visited accidentally.

You should note that, as a user of the JANET network, you must also comply with the Acceptable Use Policy of that network (<https://community.ja.net/library/acceptable-use-policy>).

PRIVACY AND CONFIDENTIALITY

Digital & Information Services makes every effort to ensure the privacy of users' data, including email messages and files held on computer systems. Email content is not viewed during the course of normal systems administration, nor are user files opened or read.

However, users should note that no absolute guarantee of privacy can be given. Operational requirements, such as action to investigate an undeliverable email message or action to recover a corrupted file, may lead to systems administrators being exposed to the content of that message or file. Where possible, users affected by such events will be notified.

Users should also be aware that emails and files stored on computers may be accessed by authorised individuals during periods of absence, for business continuity reasons. Content of emails and files stored on computers may also be examined during the course of properly authorised investigations into breaches of University policies or the law.

Any information obtained by Digital & Information Services during the course of systems administration (including monitoring) will be treated as confidential. However, users should note that where routine systems monitoring or administration indicates a breach of the University's policies or the law, Digital & Information Services will bring this information to the attention of the University or other relevant authorities.



PERSONAL USE

Reasonable personal use of the University's computer resources is permitted, but such use is subject to the University's Computer Resources - Acceptable Use Policy as well as wider University rules and regulations. Typical examples of reasonable personal use would be occasionally:

- sending emails to friends
- using the Internet for personal business or leisure, at appropriate times
- using your computer software to write a personal letter

Examples of unreasonable personal use would be:

- using the University's resources to run a commercial business concern or for-profit activity
- using a University owned computer/device for non-work purposes
- usage which brings the University into disrepute

Users should note that personal use must not interfere with the performance of duties and must not unduly impact on the resources available to others. The comments within this guide in relation to monitoring and privacy apply equally to personal use and work-related use.

SOCIAL MEDIA



The Computer Resources - Acceptable Use Policy extends to the use of University computer resources to access social media sites such as Facebook or Twitter. In addition, you must comply with the Social Media Policy for Staff (www.qub.ac.uk/home/social-media/) which covers all use of social media sites, personally and professionally.

BRING YOUR OWN DEVICE



If you use your own device, such as a smartphone or laptop to connect to the University network, or to access University systems such as email, you must adhere to the Computer Resources - Acceptable Use Policy during all such use. You must also take reasonable steps to protect any data you access.

- If you use your own mobile device or home computer for University business, you are responsible for ensuring that it has up-to-date security patches and virus protection
- You should also ensure that your device has a secure password and that 'time-out' protection, where you need to enter the password after a period of inactivity, is applied
- If you use your own device to store personal or confidential data, the data must be in an encrypted state and a risk assessment should be carried out
- 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 Policies in order to protect that data

You can report any breach of the Computer Resources - Acceptable Use Policy to the IT Service Desk (028 90973760) or by emailing cybersecurity@qub.ac.uk.

You should also inform your line manager, if appropriate.

KEEPING UP-TO-DATE WITH IT AT QUEEN'S

For more information on the IT facilities at Queen's, check out our website at www.qub.ac.uk/is. Or, to receive regular updates on the IT facilities at Queen's, you can like us on Facebook at www.facebook.com/QUBLibrary or follow us on Twitter at www.twitter.com/QUBLibrary



MAKING THE MOST OF IT AT QUEEN'S

The IT Training and Assessment Unit provides a range of courses and training materials in IT-related areas including Microsoft Office applications, SharePoint and Social Media. For more information, check out <http://go.qub.ac.uk/ittraining> or email itcourses@qub.ac.uk

www.facebook.com/QUBLibrary

www.twitter.com/QUBLibrary

www.qub.ac.uk/is