



Queen Margaret University

EDINBURGH

Information Services
and Learning
Resource Centre

**Acceptable use of information and communication
technology and electronic resources at Queen
Margaret University**

Amendment & Authorisation History

| Ver | Date | Changes | Name | Author |
|-----|----------|---|------|--------|
| A | 08/08/08 | Initial version | JR | JR |
| B | 12/08/08 | | BH | JR |
| C | 16/09/08 | Applied template, Privacy section, RIPA, changed order to bring copyright further up document | FM | FM |
| D | 27/8/09 | Added section on lecture recording | SP | FM |

[http://intranet.qmu.ac.uk/sites/is2/polpro/Acceptable use policy/Acceptable use policy for information and communication technology and electronic resources.doc](http://intranet.qmu.ac.uk/sites/is2/polpro/Acceptable%20use%20policy/Acceptable%20use%20policy%20for%20information%20and%20communication%20technology%20and%20electronic%20resources.doc)

Created by Fraser Muir

Created on 16/09/2008 11:02:00

Last saved by Fraser Muir

Last saved on 27/08/2009 12:14:00

Introduction

Queen Margaret University provides its users with access to state-of-the-art Information and Communication Technology (ICT) equipment and a wide range of electronic resources. All users need to be aware of what constitutes the Acceptable Use of these resources to enable them to be used in a safe and secure manner. This document outlines the policies relating to both ICT and e-resources and facilities.

For students, the act of matriculation at Queen Margaret University constitutes an undertaking to accept this document covering the University's ICT facilities and electronic information sources. For staff, the [Misuse of Technology Policy](#) applies.

For the purposes of this document, designations include staff and students at collaborative partners. You are reminded that accessing QMU ICT systems and resources via the Remote Desktop service you are bound by the laws and regulations in the UK as well as any applicable laws in the country from which you are connecting.

Acceptable Use Policy

1. Purpose

- The purpose of an Acceptable Use Policy is to ensure the proper use of all the University's ICT facilities and resources.
- Access to the University's ICT facilities and resources requires users to accept certain responsibilities and obligations. All users must be aware of and comply with the [JANET Acceptable Use Policy](#), which covers all UK HE academic and research network activity.
- Use of IT and associated resources should always be legal and ethical and reflect academic integrity and the standards of the University community.

2. Authorisation

In order to use the ICT facilities in the University you must first be authorised. For students, this will require your matriculation number and password, which are distributed at matriculation. Staff will receive a confidential mailing containing notification of their username and password. Your matriculation number/username and password is for the exclusive use of the individual to whom they are allocated. You are responsible and accountable for all activities carried out under your matriculation number/username and password.

3. Privacy

It should be noted that systems staff, who have appropriate privileges, have the ability, which is occasionally required, to access all files, including electronic mail files, stored on a computer which they manage. It is also occasionally necessary to intercept network traffic. In such circumstances appropriately privileged staff will take all reasonable steps to ensure the privacy of service users. The University fully reserves the right to monitor e-mail, telephone and any other electronically-mediated communications, whether stored or in transit, in line with its rights under the [Regulation of Investigatory Powers Act \(2000\)](#). Reasons for such monitoring may include the need to:

- ensure operational effectiveness of services
- prevent a breach of the law, this policy, or other University policy
- investigate a suspected breach of the law, this policy, or other University policy
- monitor standards

Access to staff files, including electronic mail files, will not normally be given to another member of staff unless authorised by the appropriate line manager, Director of IS and LRC, or nominee, who will use their discretion, in consultation with a senior officer of the University, if appropriate. In such circumstances the Head of Subject or Division, or more senior line manager, will be informed and will normally be consulted prior to action being taken. Such access will normally only be granted in the following circumstances:

- where a breach of the law or a serious breach of this or another University policy is suspected
- when a documented and lawful request from a law enforcement agency such as the police or security services has been received
- on request from the relevant Head of Subject or Division, where the managers or co-workers of the individual require access to e-mail messages or files, which are records of a University activity and the individual is unable, e.g. through absence, to provide them

The University sees student privacy as desirable but not as an absolute right, hence students should not expect to hold or pass information, which they would not wish to be seen by members of staff responsible for their academic work. In addition to when a breach of the law or of this policy is suspected, or when a documented and lawful request from a law enforcement agency such as the police or security services has been received, systems staff are also authorised to release the contents of a student's files, including electronic mail files, when required to by any member of staff who has a direct academic work-based reason for requiring such access.

After a student or member of staff leaves the University, files which are left behind on any computer system owned by the University, including servers and including electronic mail files, will be considered to be the property of the University. When leaving the University, staff should make arrangements to transfer to colleagues any e-mail or other computer-based information held under their account, as this will be closed on their departure.

4. Acceptable Use of ICT

University ICT and electronic resources are provided to facilitate your work as a member of the University community, specifically for educational, training, research or administrative purposes. Any other uses are a privilege and not a right and must never take priority over the needs of those who require the facilities for directed academic work.

QMU does not block or filter keywords or search terms, nor does it prevent you from accessing specific sites. That does not mean however, that you can access or download pornographic or other offensive or objectionable material.

You should bear the following in mind:

- You must not share your QMU username and password with anyone else. This will result in your account being disabled immediately. For students, if your account has been disabled then you must appeal for its reinstatement. This must be done in the first instance to your Dean of School. There is no automatic reinstatement. Staff should contact the IS helpdesk
- You must never use University ICT systems to alarm or inconvenience others
- You must not display anything on your screen which is likely to cause offence or upset other users. However, it is recognised that sometimes it is necessary to display material which is medical in nature, in relation to some courses/modules
- You must respect other people's electronic privacy. In particular, you may not use your QMU accounts to distribute spam and other chain emails
- For your own security, you should be careful who you share your QMU email and other contact details with

- You must never pass off other people's work as your own. The University produces a guide to referencing, "[Write and Cite](#)" which is available online
- You should not use data which is confidential or not already in the public domain in your work without first consulting the author; there may be copyright or data protection implications
- You must not maliciously damage or interfere with any item of hardware

Anyone found abusing QMU ICT systems will usually be cautioned in the first instance. Continued abuse will lead to your account being disabled. This means that you will be unable to access any of the networking and communications services. In cases of serious abuse, your account will be disabled immediately. Serious abuse includes the sharing of your username and password.

5. Forms of Unacceptable activities

Unacceptable activities can take a variety of forms. Some examples of behaviour which is unacceptable are listed below:

- Transmitting or downloading obscene or offensive material
- Transmitting or downloading threatening material, or material intended to harass or frighten
- Transmitting or downloading defamatory material
- Infringing [copyright](#) (see below)
- Hacking, attempted hacking or other deliberately disruptive activities such as introducing viruses to computer equipment
- Interfering with hardware or software configurations
- Installing or attempting to install unauthorised software to QMU ICT equipment
- Adding software to University computer equipment
- The use of QMU ICT services and equipment to distribute unsolicited advertising (*spam*), to run a business or similar activities
- Any other activities that disrupt QMU ICT services

6. Use of copyright software or datasets

By accessing QMU ICT systems, you also agree to the following with regard to copyright:

That usage of any Software, Computer Readable Dataset or Courseware or other similar material, hereafter referred to as "the Product", issued or otherwise made available to is subject to the following conditions:

- You will ensure that all the requirements of the agreements, contracts and licences under which the Product is held by the Institution will be maintained. (Copies of the relevant agreements, contracts and licences may be seen by application to the School or Department which made the Product available)
- You will adhere to the regulations governing the use of any service involved in the provision of access to the product whether these services are controlled by this institution or by some other organisation
- You will not remove or alter the Copyright Statement on any copies of the Product used by yourself
- You will ensure the Security and Confidentiality of any copy released to yourself and will not make any further copies from it or knowingly permit others to do so, unless permitted to do so under the relevant licence
- You will use the Product only for purposes defined and only on computer systems covered by the agreement, contract or licence
- You will only incorporate the Product, or part thereof, in any work, program or article produced by yourself, where this is permitted by the licence or by "Fair Dealing"

- You will only incorporate some part or version of the Product in any work produced by yourself with the express permission of the Licensor or unless this is permitted under the Agreement
- You will not reverse engineer or decompile the software products or attempt to do so unless this is explicitly permitted within the terms of the Agreement for the use of the Product

You will return or destroy all copies of the Product at the end of the course/year/period of employment or when requested to do so.

7. Legal constraints

- You must adhere at all times to appropriate statutory law such as the [Computer Misuse Act \(1990\)](#), [Theft Act \(1978\)](#), [Fraud Act \(2006\)](#), [Defamation Act \(1996\)](#) and the [Data Protection Act \(1998\)](#)
- You must undertake to comply with the [Copyright Designs and Patents Act \(1988\)](#) and the provisions of the University's licence with the Copyright Licensing Agency and with any other applicable legislation, statutory instrument or regulation
- You should always consider the provisions of the [Data Protection Act \(1998\)](#) when storing data on a computer
- You should be aware of the [Regulation of Investigatory Powers Act \(2000\)](#) when making use of ICT systems
- You must respect the intellectual property rights, copyright and moral rights of authors
- You must undertake to abide by all licence agreements for software entered into by the University with other parties (see below)
- You may only use software and/or information provided by the University for educational purposes as a member of the University

8. Code of Conduct when using our facilities

All users at QMU shall:

- Accept individual and collective responsibility for maintaining a healthy working, studying and living environment within the University, respecting the institution's policies on equal opportunities and anti-harassment and ensuring that their conduct complies with these policies
- Accept individual and collective responsibility for keeping a clean and safe working and studying environment, ensuring personal guests act in an appropriate manner. Anything which you believe constitutes a health and safety hazard must be reported immediately to Reception
- Have a mutual respect for others especially with regard to differing cultures
- Have an individual and collective responsibility to contribute to a study environment that promotes scholarship and learning. All persons should be considerate of the needs of others for an appropriate study environment and share a common goal in learning
- Have an individual and collective responsibility to ensure that the safety of themselves and others is not compromised

- Ensure that their use of the computer systems and networks is always legal and ethical and reflects academic integrity and the standards of the University community
- Have an individual and collective responsibility to ensure respect for other people and property is maintained. Eating is strictly prohibited within the Learning Resource Centre (however food may be consumed on the Terrace areas outwith the secure area of the LRC)
- Know that the use of mobile phones in lectures, seminars and computing laboratories is strictly prohibited. Mobile phones should be switched into silent mode before entering the secure area of the Learning Resource Centre. Calls must not be taken or made within this area
- Know that the University will not tolerate antisocial behaviour: this includes the use of abusive language, physical abuse, obscene comments, verbal or physical harassment and comments or remarks that discriminate on the basis of sex, race or any other irrelevant distinction

9. Penalties for unacceptable use

Infringements of this Policy will be dealt with within the University's normal disciplinary procedures – see the [Student Regulations](#) website for more information or the [Misuse of Technology Policy](#) for staff.

10. Using computers whilst on placement

Most placement organisations allow QMU users access to their ICT facilities. Make sure you know and respect their requirements on how you use their computers.

KNOW THE RULES

External organisations may have very different attitudes in the use of ICT. It is important, therefore, when you go out on a placement that you make it a priority to familiarise yourself with the local regulations. Before you go out on your placement, your academic supervisor will try to ensure that you get a copy of the organisation's specific ICT usage regulations. When you get onsite, it is worthwhile going over these regulations with your placement supervisor. This will help you get a better understanding of what is permitted and what is not. You may also find it helpful to make contact with the local ICT support department or helpdesk. The staff there will be able to give you more help and advice.

Remember – all organisations have different regulations about what you can and cannot do with their ICT facilities. You must respect these when you are out on placement. It is your individual responsibility to familiarise yourself with the local regulations and to ensure that you do not abuse the ICT facilities offered to you when you are on placement. Any computer facilities offered to you whilst on placement will be provided for University work only, i.e. for use in learning, teaching and pursuit of studies. You must not abuse these facilities for any other purpose, e.g. to play computer games, for excessive social use of email, or for recreational internet use.

KEEPING SAFE

If you are a health sciences student, your research will require internet searches based on anatomical words and phrases. This may generate unwanted links to pornographic or other objectionable websites. To be safe, read the site summary carefully before clicking on a link. If you are not sure, do not click through! Where possible, you should use specific health science related search engines.

WHAT YOU SHOULD DO IF SOMETHING UNEXPECTED HAPPENS

Even if you are careful you may accidentally access internet sites you did not mean to. This might happen because you clicked on a misleading link, you clicked on a link by accident, or because a site has been 'hijacked'. You may also find that you get bombarded by unsolicited

and explicit 'popup' advertising. If any of these things happens whilst you are out on placement:

- Take a note of the URL (web address) of the site and the time you accessed it
- Tell someone immediately. If possible, show them what happened.
- If you are working in a public area, you may want to 'lock' the PC before fetching help. (You can do this by pressing the CTRL-ALT-DEL keys at the same time, then clicking on Lock Computer. If you can't lock the PC, then make sure you have the details of the site you accessed, then log off.)
- Tell your placement supervisor as soon as possible
- Tell local ICT staff (any alerts regarding inappropriate internet use will go to them first)
- Tell your QMU supervisor to advise them of what has happened

There may be an investigation into your online activities, but if the accident was legitimate and these steps are followed, it will be resolved quickly.

11. Recording of lectures

QMU recognises that from time to time students may wish to record lectures, seminars and tutorials for their own personal use to support their learning. As a matter of courtesy students should inform the lecturer prior to the commencement of the recording. If the student has not informed the lecturer, the lecturer may ask for the recording to be stopped.

However, students are reminded that:

- Distributing a recorded lecture/seminar/tutorial is an unacceptable activity. Students should always check with lecturers before distributing a recording; this includes distributing on the Internet
- Editing a recorded lecture/seminar/tutorial is also an unacceptable activity. Students should always check with lecturers before changing a recording