

Replaces (please remove) Section 10.3 Issued 02/06

10.3 CODE OF PRACTICE FOR THE ACCEPTABLE USE OF INFORMATION AND COMMUNICATION TECHNOLOGY RESOURCES

1 PREAMBLE

The information and communication technology (ICT) resources at the University of Southern Queensland (USQ) support the instructional, research, and administrative activities of the University. Users of these facilities may have access to University resources, sensitive data, and external networks. Consequently, it is imperative for all users to behave in a responsible, ethical, and legal manner.

This document contains specific guidelines to appropriate behaviour in using USQ ICT equipment. It's purpose is to condense and present the intent of the following USQ Policies in plain language:

- USQ Policy for the Use of Information and Communication Technology Resources
- USQ Policy for Information and Communication Technology Security Management
- USQ Policy for the Use of Electronic Mail
- USQ Policy for Computer Viruses

Where appropriate, web links to supporting information are given.

2 SCOPE

These guidelines apply to all users of ICT resources and ICT equipment owned, leased or rented by University of Southern Queensland. This includes, but is not limited to:

- all students,
- academic staff,
- visiting academic staff,
- administrative staff,
- guests of University staff and
- external individuals or organisations.

ICT equipment includes, but is not limited to:

- the dialup modems,
- terminals and microcomputers in general purpose labs,
- minicomputers,
- servers, and
- networking equipment used to link these components together and to the Internet.

The University of Southern Queensland is not responsible for the content of any material you prepare, receive or transmit. Thus, as a condition of using the University's ICT facilities, you agree that you are in compliance with all Commonwealth, state and international copyright and other intellectual property laws and agreements and other Commonwealth and State laws. You also agree that in using the system you will not violate any Commonwealth or State civil or criminal laws. Furthermore, you agree to indemnify, exonerate and protect the University (and its representatives) from any claim, damage or cost related to your use of the University's ICT resources.

3 ACCEPTABLE USE

Those who make use of the USQ ICT resources are required to behave in a manner consistent with USQ's policies and codes of conduct. As a user of these resources, you agree to the following usage guidelines:

- 3.1** You are responsible for any computer account you have been given. You shall set a password on the account that is not easily guessed and shall not share this password with any other person. Guidance in setting passwords can be found at

Warning – Uncontrolled when printed. The current version of this document is kept on the USQ website.

<http://www.usq.edu.au/resources/108.pdf>. If you discover that someone has made unauthorised use of your account, you should immediately change your password and report the event to one of the individuals listed in Appendix A. You also agree not to use an account that does not belong to you.

- 3.2 You agree not to intentionally seek out information about, copy, or modify password files, other users' files, or disks belonging to other people, whether at USQ or any other facility.
- 3.3 You shall not attempt to decrypt material to which you are not entitled or attempt to gain rights you have not been specifically granted by the owner. If you observe or discover a gap in system or network security, you agree to inform the Information and Communication Technology Security Coordinator (listed in Appendix A) and not to exploit the gap.
- 3.4 You agree to refrain from any activity that intentionally interferes with a computer's operating system or its logging and security systems, or that may cause such effects.
- 3.5 You shall be sensitive to the public nature of computer systems and refrain from transmitting, posting or otherwise displaying material that is threatening, obscene, discriminating, harassing or defamatory.
- 3.6 You agree not to make copies of or distribute software the University owns or uses under license, unless permission to copy has been specifically granted by the owner of the software or the owner of the license. If in doubt as to whether you have permission to copy software, assume you don't.
- 3.7 Messages, statements, and declarations sent as electronic mail or public postings should be treated as if they were tangible documents. In a manner similar to how letterhead or a return address on a tangible document would identify the University, addressees can see that the University is the source of the message or its system is being used to transmit it, from electronic identifiers used in the transmission of messages. To make sure that no addressee can infer that your personal opinions are necessarily shared or authorised by the University, it is your obligation to clearly identify them as your opinions and not those of the University.
- 3.8 You agree not to create, alter, or delete any electronic information contained in any system associated with the University ICT resources that is not part of your own work.
- 3.9 You agree not to create, send, or forward electronic chain mail letters. You agree not to attempt to alter or forge the "From" line or any other attribution of origin contained in electronic mail or postings.
- 3.10 You shall not use USQ ICT resources as a means of obtaining unauthorised access to any other computing systems.
- 3.11 USQ's computing disk storage is a University resource with costs attached and should be used with care and discretion. It is not meant to be used for archiving programs and data not currently being used or for storage of files publicly available elsewhere. It is meant for current class work, research and development projects, and temporary storage of other files. You shall attempt to keep your disk usage minimised and will refrain from maintaining duplicate copies of software already installed on the system.
- 3.12 Network addresses such as TCP/IP addresses are assigned by the Division of ICT Services (ICT) and may not be altered or otherwise assigned without the explicit permission of the Chief Technology Officer, Division of ICT Services. In addition, no equipment may be attached to the network without the explicit permission of the Chief Technology Officer, Division of ICT Services.
- 3.13 You agree not to use the system for non University business such as the transmission of commercial advertisements, solicitations, promotions, or for reproduction of political, ideological or commercial material." Personal advertisements such as the sale of personal

items or services, of a non-commercial nature, are authorised on those forums specifically designated for such activities. Currently the only authorised forums where such activities are authorised are usq.ads, usq.books and usq.general respectively.

4 SECURITY

You should use any available methods to safeguard your data, including regular changes of passwords, making duplicates of files, and encrypting sensitive data. In the event that your files have been corrupted as a result of intrusion, you should notify the USQ Security Coordinator immediately (details in Appendix A). Please note that computer systems are not completely secure. It is possible that others will be able to access files by exploiting shortcomings in the system security. For this and other reasons, USQ cannot assure confidentiality of files and other transmissions.

The Division of ICT Services attempts to provide reasonable security against damage to files stored on USQ's computing equipment by making regular backups of systems. In the event of lost or damaged files, a reasonable attempt will be made to recover the information. However, the University and the Division of ICT Services staff cannot guarantee recovery of the data.

The Division of ICT Services will make reasonable attempts to provide error-free hardware and software on University systems, however, it is not possible to guarantee this.

5 PRIVACY

You should exercise caution when storing any confidential information in electronic format, because the privacy of such information cannot be guaranteed.

Division of ICT Services staff are expected to treat the contents of your files as private and confidential and shall not log into your account or access your files unless specifically granted permission by you, excluding the following exceptions.

Exceptions to this guideline are made under certain circumstances. These include:

- system backups, which access all files in your account;
- software upgrades which may require editing startup files in your account;
- diagnostic and trouble-shooting activities, which may, for example, require viewing the address headers of your e-mail messages to determine the cause of problems; and
- keystroke monitoring of sessions to determine inappropriate use of the computing facilities.
- suspected violation of USQ policy or local, State or Commonwealth law. If there is sufficient cause to suspect such a situation, your files may be duplicated and stored for later review by appropriate personnel without your permission.

In the event that your files need to be copied or viewed for reasons other than security, diagnostic, system backup or in compliance with law enforcement, the Division of ICT Services staff will attempt to inform you of this access.

Student staff should avoid situations where helping another student or a Faculty member would give them access to data relevant to a course that the student staff person is currently taking.

6 COPYRIGHT LAWS

Copyright is intended to provide protection for the 'intellectual property' of those people who have created something original.

If you use an image, sound, or video in a presentation, copy material produced by another person, use copyrighted text in a document, or make an extra copy of a computer program, you may be infringing copyright.

Two terms that you may come across with regard to software copyright are shareware and public domain.

6.1 Shareware

Shareware is usually software that is written and provided for evaluation purposes and can be copied and distributed. You must pay a fee to the author of the software if you intend to continue to use that piece of shareware. The software will usually contain a message that indicates where you send your fee or 'registration'. The author retains copyright of the software. Most shareware authors will send you updated or enhanced versions of the product once you are registered.

6.2 Public domain

Public domain software is available free of charge and can be copied and distributed freely. However, copyright still applies to public domain software. Therefore, if you modify and re-distribute public domain software, you must obtain permission and acknowledge the original authors.

The Australian Copyright Act 1968 and the Australian Copyright Amendment Act 1984 provide strong legal protection against unauthorised copying or use of computer software with heavy penalties that apply to individuals and organisations who breach the Act.

In brief, it is illegal:

- to copy or distribute software or any accompanying material without the permission or licence from the copyright owner;
- to run a copyrighted software program on more than one computer simultaneously unless the licence agreement specifically allows this;
- for a staff member or any section of the USQ to consciously encourage or request any staff member to make, use, or distribute illegal software copies;
- to infringe the laws against unauthorised software copying because a superior, colleague, or friend requests or compels it;
- to loan software so that a copy can be made, or to copy software while it is on loan.

7 MAIL "NETIQUETTE"

- Check your mail daily. Ignoring a mail message is discourteous.
 - Keep messages remaining in your electronic mailbox to a minimum.
 - Include your correct email address on your mail signature, business card, fax and letterhead.
 - Try to keep email messages fairly brief, a maximum of one or two full screens.
 - Make sure that the "subject" field of your email message is used and is meaningful.
 - Always reply quickly, even if a brief acknowledgement is all you can manage. At least the sender knows you have received the mail.
 - Develop an orderly filing system for those email messages you wish to keep.
 - Try to restrict yourself to one subject per message.
 - Make arrangements for your email to be forwarded to someone to handle when you go away.
 - Also remember that sending email from your USQ account is similar to sending a letter on USQ letterhead, so don't say anything that might bring discredit or embarrassment.
-
- Don't extract and use text from someone else's message without acknowledgement. This is plagiarism.
 - Don't make changes to someone else's message and pass it on without making it clear where you have made the changes.
 - Don't reproduce an email message in full when responding. Be selective in the parts that you reproduce in order to respond.
 - Don't pretend you are someone else when sending mail.
 - Don't send frivolous, foul, abusive, or defamatory messages.
 - Don't send chain letters.
 - Don't send unsolicited messages to multiple registrants on the University's mail register for purposes other than genuine university business.
 - Don't use global electronic mail for advertising or promotional purposes.
 - Don't attach excessively large files as this will result in an overflow of the disk drive of the network services provider.

Caution

Warning – Uncontrolled when printed. The current version of this document is kept on the USQ website.

It is advisable not to send confidential information that you would mind becoming public knowledge. Due to the nature of the communication medium, it is quite feasible that Internet communications may be intercepted by external entities and agencies. Also, any electronic mail that is incorrectly addressed may be received by a third person or may be bounced to a "Postmaster" in an external organisation for redirection.

8 STUDENT WEB PAGES

If you are a student of the University, personal home pages are provided as a service to you. Your published pages will be available to all users of the Internet. You must act responsibly and ensure that the content which you publish in no way breaches University policy, State or Commonwealth laws.

Student home pages will be monitored. Any person in violation of University policy will have their home page deleted and will be denied further use of this service. Further, should there be any breach of any laws, be they criminal, statutory or civil, the student who owns the pages will be held responsible, not the University.

All student home pages will have a University disclaimer automatically attached:

The University will not be responsible in any way for any damage howsoever caused to any person whatsoever in relation to any home page produced by any USQ student, or any home page accessed through USQ and which is not produced by USQ staff for the USQ.

9 VIRUSES

Clients need to consider all of the possible points of entry (Internet, email, floppy disks, personal computers, gateways, servers, staff computers connected by modems) when addressing the potential risks and implement appropriate actions to counter the risks. The success of any actions implemented depends on the detection products used and the regular use of these products by clients. As a consequence, it is imperative that you adopt a virus protection strategy and rigorously adhere to it.

9.1 Guidelines

The following guidelines are provided to assist you in implementing a successful virus protection and detection strategy. Remember that the ease with which computer viruses can be introduced onto your computer will depend on your ability to implement these simple steps.

- Scan your computer hard disk regularly for viruses using the supplied virus detection software to ensure that your computer is not infected. This check should be performed at least every week
- Identify any possible virus intrusion points where viruses are more likely to enter your computers. Implement more stringent virus scanning measures in these areas.
- Scan any floppy disks prior to using them or copying any program files contained on a floppy disk to your hard disk
- Electronic mail messages and Internet file transfers may contain files that could potentially carry viruses. Scan these files prior to using them on your computer.

If your computer is infected or you suspect that your computer may be infected by a computer virus, contact the ICT Service Desk (see Appendix A for details) immediately so that measures can be taken to remove the virus and identify any other affected computers and diskettes.

9.2 Virus Hoaxes

From time to time, email messages circulate warning of the potential virus threats. In the majority of cases, these messages are hoaxes. There is no danger associated with opening a mail message. Your computer cannot be infected in this manner. The potential danger exists only in the files and attachments that the mail message contains. Remember, always save attachments to disk and scan before executing them or opening them. If in any doubt, contact the ICT Service Desk for assistance.

10 VIOLATIONS

You should report violations immediately to any one of the individuals listed in Appendix A.

Depending on the nature of the events, violations may be dealt with as described in the USQ Handbook, any relevant contracts, and possibly State and/or Commonwealth law or regulations.

In most cases, the first action that Division of ICT Services staff will take to confirm you have violated University policy will be to close your account. To have your account reinstated, you will be required to contact ICT Services through the ICT Service Desk, to arrange an interview with the USQ Security Coordinator and/or the system administrator responsible for your case.

A senior person, such as your Dean or Head of Department, in your Department or Faculty will be informed of the circumstances of your case and any additional information arising during your interview. It is the responsibility of Faculties or Departments to impose appropriate disciplinary penalties, including any extension of closure of your account.

11 FREQUENTLY ASKED QUESTIONS

If you have any questions concerning the use of computer systems at USQ you should contact ICT staff at the ICT Service Desk (see Appendix A for details)

Another useful source of answers to “Frequently Asked Questions” are the FAQ’s compiled by ICT staff.

- Staff members should link to <http://www.usq.edu.au/currentstaff/resources/default.htm>
- Students should link to <http://www.usq.edu.au/> and use their user name and password to log on.

12 APPENDIX A**Division of ICT Services****USQ Security Coordinator**

Les Mitchell

Manager (Business Continuity and Risk Manager)

Division of Information and Communication Technology Services

ICT Performance Measurement & Investment Management

Ph: (07) 4631 2483

mitchell@usq.edu.au

ICT Service Desk**USQ Support Centre, Y Block**

Division of ICT Services

Ph (07) 4631 1900

ictservicedesk@usq.edu.au