

(Regulation) ICT Code of Practice for the Acceptable Use of ICT Resources

Document Purpose

Document Purpose	<p>This document contains specific guidelines to appropriate behaviour in using USQ ICT Resources.</p> <p>The purpose of this document is to condense and present the intent of all relevant USQ ICT standards in plain language.</p>			
Document Information	Version	1.1		
	Release Date	November 2009		
	Release Status	Final		
	Review Date	November 2010		
	Author(s)	Principal Manager – Service Delivery		
	Owner	Principal Manager – Service Delivery		
	Print Date	Last Printed: 9/11/2009 2:35:00 PM		
	Approved By	Principal Manager – Service Delivery		
	Policy	USQ Policy for ICT Information Management and Security		
	Type of Document	Regulation		
	Electronic Location and Filename	http://www.usq.edu.au/~media/USQ/ICT/ICTCodeofPracticefortheAcceptableUseofICTResourcespdf.ashx		
Version Control	Version	Date	Author(s)	Summary of Changes
	0.1	Jan/ June 2008	Various	Document creation
	1.0	Jul 2008	Maggie Fryer	Final Release
	1.1	Oct 2009	Michael Thompson	New Section (11) "Using Mobile Devices"
Error Advisory	<p>To the Reader:</p> <p>If you encounter any inaccuracies or printing faults in this document please contact the Owner (see Document Information section, above) as soon as possible. The Owner will then initiate the required modifications</p> <p>If you are unable to contact the Owner, contact that person's Manager Supervisor.</p> <p>Thank you for helping the Division of ICT Services maintain quality documentation.</p>			

Table of Contents

Document Purpose	1
Document Information	1
Error Advisory	1
1 Definitions	3
2 Introduction	3
3 Scope	4
4 Acceptable Use	5
4.1 Authorised Use.....	5
4.1.1 Limited Personal Use*.....	5
4.2 Unauthorised Use.....	6
4.2.1 Unauthorised Personal Use	6
5 Security	8
6 Privacy	9
7 Copyright	10
8 Email	11
8.1 Standard Disclaimers - Email	12
9 Web Pages	13
10 Malware (Viruses and Spyware)	14
10.1 Guidelines	14
11 Using Mobile Devices	15
12 Violations	16
13 Frequently Asked Questions	16
14 Related Documents	17
15 Appendix A	18

1 Definitions

The [ICT Glossary and Definitions](#) contains a description of any common ICT terminology referred to in the policy and standard documentation.

2 Introduction

The information and communication technology (ICT) resources at the University of Southern Queensland (USQ) support the corporate goals of the University as outlined in the USQ Strategic Plans. Clients may have access to University resources, sensitive data, and external networks.

Consequently, it is imperative for all clients to behave in a responsible, ethical, and legal manner to ensure the integrity, security, and availability for appropriate educational, learning, and business activities conducted by the University.

3 Scope

These guidelines apply to all clients of ICT resources and ICT equipment owned, leased, or rented by the University of Southern Queensland and includes use at home. It also applies to any person connecting personally owned equipment to the University network from any location. This includes, but is not limited to:

- All students.
- Academic staff.
- Visiting academic staff.
- Administrative staff.
- Guests of University staff.
- External individuals or organisations.

ICT equipment includes, but is not limited to:

- Dialup modems, wireless access cards and network interfaces.
- Desktop, notebook, tablet, mobile phones and personal digital equipment.
- Peripheral devices such as printers, scanners.
- Servers.
- Networking equipment and communications networks used to link these components together and to the Internet.

The University of Southern Queensland is not responsible for the content of any material prepared, received, or transmitted by Clients.

As a condition of using the University's ICT resources, you agree that you will comply 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.

Use of ICT facilities is at all times subject to the conditions and constraints relating to their use in terms of University security, privacy, copyright, confidentiality, and delegation policies, standards, and guidelines.

4 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 regulations:

4.1 Authorised Use

- 1 You are responsible for the use of any computer account you have been given. You shall set a password on the account that is not easily guessed and you shall not share this password with any other person. Guidance in setting passwords can be found in the [ICT Standard for Computer Passwords and Access Controls](#).
 - i. 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.
- 2 If you observe or discover a gap in system or network security, you agree to inform the Information and Communication Technology Security Officer (listed in Appendix A) and not to exploit the gap.
- 3 Messages, statements, and declarations sent as electronic mail or public postings should be treated as if they were tangible documents.
 - i. 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.
 - ii. 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.
- 4 USQ's computing network usage and disk storage are University resources with costs attached and should be used with care and discretion. Storage is not meant to be used for archiving programs and data not currently being used, or for storage of files publicly available elsewhere. Storage is meant for current course work, research and development projects, and temporary storage of other files.
 - i. You shall attempt to keep your disk usage minimised and will refrain from maintaining duplicate copies of software already installed on the system.

4.1.1 Limited Personal Use*

University ICT resources, including internet, telephony, instant messaging and email services, are provided for University business, but limited personal use is allowed.

'Limited personal use' means use that is infrequent and brief. This should generally occur during personal time and should not include:

- Use that takes a lot of time.
- Private business that is for personal gain or profit.
- Items that interfere with USQ Information Communication Technology.
- Clogging mailboxes with large numbers of messages.
- Violating policies, standards, legislation, or regulations.
- Violating this Code of Practice.

As a guide, use that occurs more than a few times per day and/or for periods longer than a few minutes would not be considered limited personal use.

Clients may be held personally responsible for any use of ICT resources that does not comply with these principles.

The University accepts no liability for any loss or damages suffered by users as a result of personal use.

*Any exemptions to this clause will be outlined in the [ICT Standard for the Use of ICT Resources](#).

4.2 Unauthorised Use

- 1 You agree not to use a computer account that does not belong to you.
- 2 You agree not to intentionally seek out information about, copy, or modify password files, other clients' files, or disks belonging to other people, whether at USQ or any other facility.
- 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.
- 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.
- 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.
- 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.
- 7 You agree not to create, alter, or delete any electronic information contained in any system associated with University ICT resources that is not part of your own work.
- 8 You shall not use USQ ICT resources as a means of obtaining unauthorised access to any other computing systems.
- 9 Network addresses such as TCP/IP addresses are assigned by the Division of ICT Services (DICTS) and may not be altered or otherwise assigned without the explicit permission of the Chief Technology Officer or delegated officer, Division of ICT Services.
- 10 In addition, no equipment may be attached to the network without the explicit permission of the Chief Technology Officer or delegated officer, Division of ICT Services.
- 11 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.
- 12 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. Staff are referred to the University's Extra Remunerative Activity Policy and to the University's Code of Conduct.
- 13 You agree not to intentionally access, download, store, or distribute material of a pornographic nature other than with the approval from an authorised University Officer for research related purposes.
- 14 You agree not to perform any monitoring, scanning or "sniffing" of the University ICT network unless authorised by the Chief Technology Officer or delegated officer, Division of ICT Services.

4.2.1 Unauthorised Personal Use

Unauthorised use of Information Communication Technology includes, but is not limited to:

- Infringing the copyright or other intellectual property right of the University or third parties.
- Scanning and/or printing resources protected by copyright.
- Disrupting communication and information devices through such means as mass emailing or transmitting files which place an unnecessary burden on University resources.
- Engaging in any illegal or wrongful activity.
- Engaging in private business or personal profit ventures.
- Disrupting or interfering with the use of Information Communication Technology.

- Effecting security breaches of network communication - security breaches include, but are not limited to, accessing data of which the client is not an intended recipient, and logging in to a server or account that the client is not authorised to access.
- Executing any form of unauthorised network monitoring.
- Circumventing user authentication or security of any host, network, or account.
- Without authority: destroying, altering, dismantling, disfiguring, preventing rightful access to, or otherwise interfering with, the integrity of Information Communication Technology.
- Accessing offensive internet sites.

Clients may not use internet or email access to:

- Download, distribute, store or display pornographic and other offensive graphics, images or statements, or other material obtained from offensive internet sites.
- Download, distribute, store or display material that could cause offence to others (for example, offensive material based on sex, gender, ethnicity or religious and political beliefs).
- Download large amounts of material for personal use.
- Download information for external organisations or the general public, without authorisation.
- Distribute chain letters.
- Distribute defamatory, obscene, offensive, or harassing messages.
- Distribute confidential information without authority.
- Distribute private or personal information about other people without authorisation.
- Distribute messages anonymously, using a false identity, or using another person's user or email details.

5 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 ICT Security Officer immediately (details in Appendix A).

Please note that computer systems and the Internet 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.

All PCs, laptops and workstations should be secured with a password-protected screensaver, with the automatic activation feature set at 15 minutes or less (or by logging off when the equipment will be unattended).

Because information contained on mobile computing equipment such as laptops is especially vulnerable, special care should be exercised. Where mobile computing equipment is not taken home after hours, USQ users are responsible for ensuring that this equipment is secured in a locked room or container.

6 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
- Keystroke monitoring of sessions to determine inappropriate use of the computing facilities;
- Suspected violation of USQ policy and standards 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 shall 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.

7 Copyright

The Copyright Act sets out the exclusive rights of copyright owners and is intended to provide protection for the 'intellectual property' of those people who have created something original as well as specifying the rights of users.

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.

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 that 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.

8 Email

Guidance in using electronic mail can be found in the [ICT Standard for the Use of Electronic Mail](#).

- 1 You must not express views on behalf of the University without official authorisation, or to allow another person to reasonably believe that a personal view represents the official position of the University. In circumstances where readers of your electronic communication might reasonably conclude that a personal view is representative of the University, it is your obligation to clearly state and identify that the opinions expressed are those of the author, and not necessarily those of the University, or words to that effect.
- 2 The "#USQ EXECUTIVE COMMUNIQUE" mailing list is only to be used by authorised staff for the distribution of official USQ email messages to the University staff community. Alternative mailing lists, which staff can opt to subscribe to or unsubscribe to, are available for the specific purpose of providing a mechanism to distribute un-official email messages to the University staff community.
- 3 You agree not to replicate the "#USQ EXECUTIVE COMMUNIQUE" by assembling the various mailing lists that comprise this master mailing list in the "To" line for the purposes of distributing un-official messages and circumventing gaining approval from the official authorised staff.
- 4 You agree not to create, send, or forward electronic chain mail letters or knowingly distribute spam emails.
- 5 You agree not to attempt to alter or forge the "From" line or any other attribution of origin contained in electronic mail or postings.
- 6 You agree not to send anonymous email messages.
- 7 You agree to only send messages to a University electronic mailing list that are relevant to the membership of the list.
- 8 If you receive inappropriate material through email, immediately delete the email (and any attachments) from the University's systems.
- 9 Check your email daily. Ignoring an email message is discourteous.
- 10 Keep messages remaining in your electronic mailbox to a minimum.
- 11 Include your correct email address on your mail signature, business card, fax and letterhead.
- 12 Try to keep email messages fairly brief, a maximum of one or two full screens.
- 13 Make sure that the 'Subject' field of your email message is used and is meaningful.
- 14 Always reply quickly, even if a brief acknowledgement is all you can manage. At least the sender knows you have received the email.
- 15 Develop an orderly filing system for those email messages you wish to keep.
- 16 Try to restrict yourself to one subject per message.
- 17 Make arrangements for your email to be forwarded to someone to handle when you are away from campus.
- 18 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.
- 19 Do not extract and use text from someone else's message without acknowledgement. This is plagiarism.
- 20 Do not make changes to someone else's message and pass it on without making it clear where you have made the changes.
- 21 Do not reproduce an email message in full when responding. Be selective in the parts that you reproduce in order to respond.
- 22 Do not pretend you are someone else when sending email.
- 23 Do not send frivolous, foul, abusive, or defamatory messages.
- 24 Do not send chain letters.
- 25 Do not send unsolicited messages to multiple registrants on the University's mail register for purposes other than genuine University business.
- 26 Do not attach excessively large files as this will result in an overflow of the disk drive of the network services provider.

8.1 Standard Disclaimers - Email

The following disclaimer is automatically included at the end of the signature block of email messages sent outside the USQ:

“This email (including any attached files) is confidential and is for the intended recipient(s) only. If you received this email by mistake, please, as a courtesy, tell the sender, and then delete this email.

The views and opinions are the originator's and do not necessarily reflect those of the University of Southern Queensland. Although all reasonable precautions were taken to ensure that this email contained no viruses at the time it was sent we accept no liability for any losses arising from its receipt

The University of Southern Queensland is a registered provider of education with the Australian Government (CRICOS Institution Code No's. QLD 00244B / NSW 02225M)”

9 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."

10 Malware (Viruses and Spyware)

Clients need to consider all of the possible points of entry (internet, email, removable media, personal computers, gateways, servers, staff computers connected by modems) when addressing the potential risks, and implement appropriate actions to counter those 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 malware protection strategy and rigorously adhere to it.

10.1 Guidelines

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

- Scan your computer hard disk regularly for malware 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 malware is more likely to enter your computers. Implement more stringent virus scanning measures in these areas.
- Scan any removable media 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 malware. 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 malware, contact the ICT Service Desk (see Appendix A for details) immediately so that measures can be taken to remove the malware and identify any other affected computers and storage media.

11 Using Mobile Devices

Clients need to be aware of the specific risks that apply regarding the use of mobile devices. The following guidelines are provided to assist clients comply with good practice.

- Personal computers should not be used at home for business activities if virus controls are not in place.
- When travelling, ICT equipment and media should not be left unattended in public places. Portable computers should be carried as hand luggage when travelling.
- Tim-out protection should be applied.
- Portable and attractive items such as portable computers, mobile phones, pdas and digital cameras are vulnerable to theft, loss or unauthorised access when travelling. They must be provided with an appropriate form of access protection (eg. Passwords and/or encryption) to prevent unauthorised access to their contents.
- Passwords or other access tokens for access to the University's ICT systems should never be stored on mobile devices where they may be stolen and give the thief unauthorised access to information assets.
- Manufacturer's instructions regarding the protection of equipment should be observed at all times.
- Security risks (eg. of damage, theft) may vary considerably between locations and this should be taken into account when determining the most appropriate security measures.

(Note: most of these guidelines are attributed to "Universities and Colleges Information Systems Association (UCISA) Toolkit Information Security Edition 3.0")

12 Violations

You should report violations immediately to any one of the individuals listed in Appendix A. Penalties and Disciplinary action are outlined in Section 8 of the *USQ Policy for ICT Information Management and Security*.

In most cases, the first action that Division of ICT Services staff will take to confirm that 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 ICT Security Officer and/or the Corporate Executive Portfolio Steward/ Principal Activity Steward/System Sponsor or their delegated officer responsible for your case.

13 Frequently Asked Questions

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

14 Related Documents

Document (Electronic)	Australian Copyright Act 1968 available at http://www.austlii.edu.au/au/legis/cth/consol_act/ca1968133/
Document (Electronic)	Australian Copyright Amendment Act 1984 available at http://www.comlaw.gov.au/comlaw/Legislation/Act1.nsf/0/2FD6608D8AB56D1ACA256F72001595D7?OpenDocument
Document (Electronic)	ICT Standard for Computer Passwords and System Access Controls available at http://www.usq.edu.au/~media/USQ/ICT/ICTStandardforComputerPasswordsandSystemAccessControlspdf.ashx
Document (Electronic)	ICT Standard for the Use of Electronic Mail available at http://www.usq.edu.au/~media/USQ/ICT/ICTStandardfortheUseofElectronicMailpdf.ashx
Document (Electronic)	ICT Standard for the Use of ICT Resources available at http://www.usq.edu.au/~media/USQ/ICT/ICTStandardfortheUseofICTResourcespdf.ashx
Document (Electronic)	Spam Act 2003 (Cth) available at http://scaleplus.law.gov.au/html/comact/11/6735/pdf/1292003.pdf

15 Appendix A

Division of ICT Services

ICT Security Officer

Division of Information and Communication Technology Services

Ph: (07) 4631 2877

ICT Service Desk

E Block Reception, Toowoomba Campus

Division of ICT Services

Ph (07) 4631 1900

ictservicedesk@usq.edu.au