

(Standard) ICT Standard for the Use of ICT Resources

Document Purpose

Document Purpose	To ensure ICT Resources are used only in a manner consistent with the goals of the University.			
Document Information	Version	1.0		
	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: 28/07/2010 3:58:00 PM		
	Approved By	Principal Manager – Service Delivery		
	Policy	USQ Policy for ICT Information Management and Security		
	Type of Document	Standard		
	Electronic Location and Filename	http://www.usq.edu.au/ict/standards/ict_standard_for_the_use_of_ict_resources.pdf		
Version Control	Version	Date	Author(s)	Summary of Changes
	0.1	2008	Various	Document creation
	1.0	July 2008	Maggie Fryer	Final release
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 of Information Technology Services	4
3.1 Responsibility With Regard to Australian Laws, USQ Policies and Contracts Between the University and External Agencies	4
4 Standards.....	6
4.1 Acceptable Use.....	6
4.2 Identity Management	6
4.3 Privacy.....	6
4.4 Network Integrity.....	6
4.5 Standard Office Computing Environment	7
4.6 Defamation, Harassment and Other Abusive Behaviour	7
4.7 Illicit Material.....	7
4.8 Copyright	7
4.9 Knowledge of Breach of Standard	7
4.10 Disciplinary Action	7
5 Regulations.....	8
5.1 Acceptable Use.....	8
5.2 Authorised Clients.....	8
5.2.1 Registration of Clients	8
5.2.2 Cancellation of Registration	9
5.3 Security.....	9
5.4 Use of University Property	10
5.5 Official Representation of the University	10
5.5.1 Expression of Personal Views	10
5.6 Electronic Communications and Online Content.....	11
5.7 Interference or Monitoring Other Clients.....	11
5.8 Malware (Viruses and Spyware).....	11
5.8.1 Guidelines	11
5.9 Mobile Devices	12
5.10 Frequently Asked Questions.....	12
6 Related Documents.....	13
7 Appendix A	14

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 University has identified the pivotal role of Information and Communication Technology (ICT) to enhance the academic programme and support services available to staff, students and alumni (hereinafter referred to as clients). The University Strategic Plan articulates a number of key goals and strategies that direct how computing equipment, networks, systems and software (hereinafter referred to as ICT Resources) will be employed to improve instructional systems, information systems, and communications services for clients.

Each member of staff is provided with convenient access to a computer workstation networked to a wide variety of electronically based services available on campus, and other services accessible across the Internet. Extensive training and support services are provided to ensure these resources are used effectively. Student facilities are regularly upgraded to ensure the needs of the academic programme are met.

The University authorises clients to access ICT Resources appropriate to their needs. All persons have a responsibility to use these facilities in a responsible and considerate manner. This standard has been formulated with the view of creating an environment where clients as users of ICT Resources made available by the University have an understanding of their responsibilities, duties and obligations.

3 Scope of Information Technology Services

The University provides ICT Resources that are consistent with the mission and goals of the University. Specifically, services are provided which support the corporate goals of the University as outlined in the USQ Strategic Plans.

This standard applies 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 and alumni,
- Academic and administrative staff,
- Visiting academic staff, and
- 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, and
- 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 not violate any Commonwealth or State civil or criminal laws, and that you will comply with all Commonwealth, State and international copyright and other intellectual property laws and agreements and other Commonwealth and State 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.

3.1 Responsibility With Regard to Australian Laws, USQ Policies and Contracts Between the University and External Agencies

The University has obligations relating to intellectual property, sexual harassment, and racial discrimination as defined by law, and in its own policies.

The University expects that users of its ICT Resources will also exercise their responsibilities in this area.

Clients should familiarise themselves with University policies and documentation on the following matters:

- [Code of Conduct \(Human Resources Policy and Procedures Manual, Part C1\)](#),
- [Intellectual Property \(University Calendar, Sections 7.9\)](#),
- [Copyright \(University Calendar, Section 7.10\)](#),
- [Anti Discrimination policy](#),
- [Sexual Harassment policy](#), and
- [Racial Discrimination policy](#).

Clients must not act fraudulently in any way, for example, making false representations about any matter, or about the authorship of any document or work, or falsely attributing the source of any material to another person, or forging anything.

The University has certain contractual obligations relating to the use of its ICT Resources which constrain the way facilities may be used. The University may take disciplinary action against anyone whose use of facilities violates the terms of such agreements. In addition to observing Australian laws, related USQ policies and standards, and this standard, clients should familiarise themselves with any published acceptable use standard associated with each service.

4 Standards

4.1 Acceptable Use

The University's ICT environment is dynamic, characterised by openness, creativity and free sharing of information, to the greater benefit of universities generally. This standard will respect this environment and inhibit these characteristics only when necessary to protect the essential interests of the University.

University ICT resources, including internet, telephony, instant messaging and email services, are provided for the purposes of conducting University business. It is acknowledged that limited personal use will occur. 'Limited personal use' means private use that is infrequent and brief. The University accepts no liability for any loss or damages suffered by users as a result of personal use.

4.2 Identity Management

The University Identity Management System (IDM) is responsible for the overall management and security of staff, student and pseudo accounts. Academic and administrative staff will be authorised to access resources required to perform their duties. Students will be authorised to access services for academic purposes relating to their program of study at the University. Alumni will be authorised electronic mail and any other resources allocated to them. Clients who are not staff, students or alumni may have pseudo or affiliate account access provided.

4.3 Privacy

The University of Southern Queensland recognises the right to privacy of client files and communications. However, the University reserves the right to examine files and directories where it is necessary to determine the ownership or recipient of lost or misdirected files, and also where the University has information or evidence that:

- System integrity is threatened,
- Security is compromised,
- An activity has a detrimental impact on the quality of service to other clients,
- The system is being used for purposes which are prohibited under this standard, or
- The system is being used for unlawful purposes

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

4.4 Network Integrity

The campus computer network is recognised as a key element of the electronic based services that support the academic programme.

Computers may be connected to the network only in accordance with the [ICT Standard for Physical and Environmental Security](#) and associated standards. Systems must be registered and allocated an appropriate network address which is compatible with all other equipment and systems associated with the network.

Any form of experimentation with the campus network is prohibited.

4.5 Standard Office Computing Environment

A standard suite of office applications software is adopted in order to maximise benefits to the University community in the form of improved communications, training materials and technical support services for clients with workstation connections to the campus network.

4.6 Defamation, Harassment and Other Abusive Behaviour

No client will, under any circumstances take any action which would or might lead to the University's ICT Resources being used for the purpose of defaming or slandering any individual or organisation or use an ICT system in any way such that a reasonable individual may consider this action to be viewed as harassing, abusive or obscene behaviour.

4.7 Illicit Material

No client will, under any circumstances use the University's ICT Resources to access, transfer, or store illicit material.

4.8 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.

4.9 Knowledge of Breach of Standard

Should any client become aware of any action by another individual which could be considered to breach this standard, they are requested to take appropriate action to ensure it is brought to the attention of ICT management.

4.10 Disciplinary Action

Penalties and Disciplinary action are outlined in Section 8 of the *USQ Policy for ICT Information Management and Security*.

5 Regulations

5.1 Acceptable Use

Unauthorised use of any USQ ICT resource is not permitted. 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:

1. You are responsible for the use of any computer account you have been given. You shall set and use 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](#).

If you discover that someone has made unauthorised use of your account, you should immediately change your password and report the event to the Division of ICT Services.

2. Any gap in system or network security should be reported immediately to the Division of ICT Services.
3. Electronic mail and online postings should be treated as if they were tangible documents. Staff members are reminded to distinguish between personal opinion and authorised University statements when communicating electronically or online and should ensure that no addressee can infer that your personal opinions are necessarily shared or authorised by the University. In these circumstances, it is a staff member's obligation to clearly identify them as their opinions and not those of the University.
4. USQ's computing network and internet usage and disk storage are not unlimited University resources. Quotas for storage and internet traffic should be adhered to ensure that associated usage costs are sustainable.

5.2 Authorised Clients

Access to the University's ICT Resources is for authorised staff, students, alumni and third parties (affiliates and pseudo).

Persons other than staff, students and alumni may be provided access to use ICT Resources under special circumstances consistent with other policies of the University and subject to appropriate authorisation and indemnities.

Clients are responsible for the use of their own accounts and are permitted to access only those resources for which they have been authorised. No client may use any other client's authorisation to access any system or allow any other person to use their authorisation to access any system.

5.2.1 Registration of Clients

The Identity Management System (IDM) is the access control system used to automate the creation of client accounts to access USQ computer systems and ICT resources. As new systems are introduced and existing systems updated, the intention is to progressively migrate all ICT resource access registration processes through IDM. Provisioning of resource access to a client account is allocated on the basis of a client's classification (eg. staff, student, third party).

Where registration processes exist, responsibility for defining and managing any registration processes that may apply in regard to access will reside with the designated Corporate Executive Portfolio Steward/ Principal Activity Steward/System Sponsor responsible for that ICT Resource.

Staff

All academic and general staff must be authorised to access ICT Resources identified and agreed by their delegated officer as being required to perform their duties, provided this is in accordance with other University policies, and subject to authorisation being confirmed by the University's delegated officer in the department nominated as managing the facility on behalf of the University.

Students

All students will be authorised to access ICT resources required to undertake their course of study. Students may be registered to access additional ICT Resources like the general purpose microcomputer laboratory facilities and/or to access a common set of electronic or online services that will provide them with an information rich learning environment.

Students may be registered as users of other ICT Resources, provided it is a genuine requirement of their academic studies, as detailed in a unit specification, or authorised by their Dean or delegated officer as being required to complete their studies, provided this is in accordance with other University policies, and subject to authorisation being confirmed by the University's delegated officer in the department nominated as managing the facility on behalf of the University.

Third Parties and Visitors

Third parties and visitors will be allocated a pseudo or affiliate user account. Such access may be authorised to access ICT Resources in accordance with other University policies, and subject to:

- The authorisation of the appropriate Dean or delegated officer and
- Subject to authorisation being confirmed by the University's delegated officer in the department nominated as managing the ICT resource on behalf of the University.

5.2.2 Cancellation of Registration

Student portal access is intended to be granted for life.

Staff registrations will be disabled on their last day of employment or the resource access is no longer required to perform their duties.

Any client may have his/her registration(s) terminated or suspended for breach of any of the terms of this standard or related standards, as determined by the Dean or delegated officer responsible for the client and the Corporate Executive Portfolio Steward/ Principal Activity Steward/System Sponsor responsible for managing the ICT resource in question.

5.3 Security

The primary means of security for the University's ICT Resources is through the allocation of individual computer accounts and access passwords (Refer to the [ICT Standard for Computer Passwords and System Access Controls](#)). It is every client's responsibility to ensure that:

- Passwords are selected carefully and not shared with other persons,
- Computer workstations are kept physically secure, and
- Computer accounts are not shared with other persons.

No client will, under any circumstances, take any action which would or might lead to circumventing or compromising security of any of the University's ICT Resources).

A client 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).

You are advised 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.

All desktop computers, laptops and computer 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).

Information contained on mobile computing equipment such as laptops is especially vulnerable and 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.

5.4 Use of University Property

The University's ICT Resources, as with other University resources, are not to be used for purposes other than those deemed appropriate by the University as defined in the [USQ Financial Management Practices Manual \(Part Five\)](#). It is recognised that "limited personal use" will occur and cannot be totally eliminated. Excessive personal use is not appropriate.

On the whole it is expected that staff will not use the University's ICT Resources for private purposes and students may not use the University's ICT Resources for purposes other than those directly related to their studies except on designated systems.

An exemption to this provision will occur where a commercial agreement exists between clients residing in facilities and the University, such as the Residential Colleges, and ICT Resources are provided as part of a commercial agreement between the parties. The University accepts no liability for any loss or damages suffered by the client as a consequence of this personal use.

5.5 Official Representation of the University

Clients must be aware that the correspondence and discussion into which they enter when using the University network and the Internet may be construed to be representative of the University's position.

Where the client is representing the views of the University, then a notation must be appended to the communication identifying the individual and the position title held within the University.

5.5.1 Expression of Personal Views

Where the client does not have authority or is not aware of the University's position or where their personal view may vary from that of the University such correspondence must clearly state that the opinion expressed is that of the writer, and not necessarily that of the University, or words to that effect.

5.6 Electronic Communications and Online Content

Facilities for electronic communications (such as electronic mail, blogs, wikis, list servers and news) are provided for general use consistent with this and other University policies.

If you are a student of the University, ePortfolio space and personal home pages are provided as a service to you. Your published online content will be available to other Internet users. 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 relevant law, 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."

5.7 Interference or Monitoring Other Clients

No client will, under any circumstances, take any action which would or might lead to denial of service or impairment of access to or effective use of, any ICT resource by any other authorised client.

No client will, under any circumstances, take any action to monitor the network or segments of the network in order to intercept the communications being sent to or from a client on the USQ network unless such monitoring is authorised.

The promulgation of software viruses or similar contaminant software is expressly forbidden.

5.8 Malware (Viruses and Spyware)

Clients need to consider all of the possible points of malware 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.

5.8.1 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.

5.9 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.
- Time-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

5.10 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).

6 Related Documents

Document (Electronic)	University Strategic Plan http://www.usq.edu.au/planstats/Planning/
Document (Electronic)	USQ Financial Management Practices Manual http://www.usq.edu.au/financialservices/policies/financialpractice.htm
Document (Electronic)	USQ HR Policies and Procedures Manual – Code of Conduct http://www.usq.edu.au/hr/polproc/partc/c6.htm
Document (Electronic)	Intellectual Property Policy http://www.usq.edu.au/hr/polproc/partc/c1.htm
Document (Electronic)	Copyright Statement http://www.usq.edu.au/legaloffice/copyright/default.htm
Document (Electronic)	Anti-Discrimination Statement http://www.usq.edu.au/legaloffice/antidiscrim.htm
Document (Electronic)	Anti-Discrimination and Freedom from Harassment Policy http://www.usq.edu.au/hr/polproc/partc/c2.htm
Document (Electronic)	ICT Standard for Computer Passwords and System Access Controls http://www.usq.edu.au/resources/ict_standard_for_computer_passwords_and_system_access_controls.pdf
Document (Electronic)	ICT Standard for Physical and Environmental Security http://www.usq.edu.au/resources/ict_standard_for_physical_environment_security.pdf

7 Appendix A

Division of ICT Services

ICT Security Officer

Division of Information and Communication Technology Services

Ph: (07) 4631 2877

ICT Service Desk

USQ Support Centre, Toowoomba Campus

Division of ICT Services

Ph (07) 4631 1900

ictservicedesk@usq.edu.au