

GUIDELINES – UQ GUIDELINES IN THE USE OF UQ INFORMATION, COMMUNICATION AND TECHNOLOGY (ICT) RESOURCES

1. PURPOSE

The University of Queensland's information, communication and technology (ICT) facilities is provided to the University to support the University's teaching and learning, research and community service activities. In order for staff and students and other associated authorised users to take full advantage of these facilities for these purposes, responsible use is expected.

The purpose of this guideline is to:

- Provide information on how to use the computing and network facilities responsibly.
- Provide information on where to find relevant UQ policies with respect to the use of UQ resources
- Provide guidelines for what to do in the event that inappropriate use of UQ IT resources by UQ staff and students is discovered or reported.

Access by authorised users to the UQ computing and networking facilities imposes certain responsibilities and obligations and access is granted subject to policies and statutes of the University, and state and federal laws. Use of ICT facilities for illegal activities, accessing gambling internet sites, or downloading and distributing copyrighted material without permission will not be tolerated.

2. GUIDELINES OF USE

Access

- **Use for UQ purposes:** As stated in the Internet Code of Practice, the "University's network can be used only by University staff, students and associated individuals (eg visiting fellows honorary research associates) and only for, or in connection with, the research, educational or administrative functions of the University". The network can be used for personal use where it is kept to a minimum (see section below)

Access to authorised community users is also provided.

- **Authorised Accounts:** Access to the UQ network will be by an authorised account. Computers in the Library, are exempt where the internet access is limited to "the trusted zone".
- **Non-sharing of Account Details:** Staff should not share their account details with other staff or write passwords down where they are easily accessible and used by another person.
- **Use within the Law, Codes and Standards:** Users of UQ resources must not breach any laws, codes, standards, and content requirements of any relevant authority
- **Permission for Under 18s:** The Telecommunications Act 1997 and the Broadcasting Services (Online Services) Act 1999 prohibit the University from providing unsupervised access to the Internet to anyone under the age of 18 without evidence of consent by their parent or legal guardian. [Under 18 Internet Access Permission forms](#) are available from the UQconnect website.

Unacceptable Use

The following areas outline what may be considered inappropriate use of ICT resources. In instances where downloading is required for legitimate research or teaching purposes, an exception may apply

- **Destruction & Damage to IT resources:** Destruction of, or damage to equipment, software, or data belonging to the University of Queensland or other clients.
- **Unauthorised Access/Hacking:** Attempts to gain unauthorised access to computer network systems
- **Unauthorised Monitoring:** Unauthorised monitoring of electronic communications. (Authorisation for monitoring is required from the Director, ITS for security purposes.)
- **Offensive and Inappropriate Material:** Knowingly downloading, storing, distributing and viewing of offensive, obscene, indecent, pornographic, or menacing material. This could include, but not limited to pornography, hate sites, gratuitous violence and sites using frequent and highlighted bad language.

- **Unauthorised Copyright Material including Software:** Unauthorised Acquisition, reproduction, distribution and use of copyrighted material is illegal without written permission of the owner. Software may not be used or downloaded unless appropriate licensing conditions are met.
- **Music/Movies** Downloading and storage of material such as music/movie clips requires use of considerable UQ resources and as such is unacceptable unless required for University purposes and within copyright. Broadcasting or creating fileshares for such material is also unacceptable unless it is for University Purposes.
- **Peer to Peer File Sharing:** Use of Peer to Peer (P2P) files sharing software can be a significant security threat to the University as well as posing a threat to network bandwidth and download misuse and legal liability. P2P is not permitted to be used on any UQ facilities unless it has been approved by the Head of an organisational unit as legitimate use and notification has been given to the Director, ITS, who would maintain a register of approved systems. Examples of these applications are KaZaA, Gnutella, iSwipe, MLDonkey Lime Wire, Shareaza, Morpheus, BearShare and eDonkey.
- **Gambling:** The accessing of gambling internet sites is unacceptable.
- **Games:** Playing of games is not permitted by staff within work hours. Students should also not use UQ resources for playing games unless it is a legitimate requirement of their studies. The loading of privately owned games software, breaches the UQ Internet Code of Practice. Games can require a large amount of internal storage and potentially long play periods breaching the UQ minimal use standard. The loading of such software also potentially has software licensing and security concerns.
- **Date/match-making:** The accessing of date/match making sites is inappropriate in a work and student environment.
- **Inappropriate Screen Savers/Wallpapers:** Screen Savers and wallpapers that could be considered of an offensive nature are inappropriate in a work environment.
- **Unlicensed Software:** Software may be downloaded for University purposes. All licensing conditions however must be adhered to with regard to its evaluation and subsequent use
- **SPAM:** Mass emailing across UQNet and the internet (SPAM) is not permitted except as defined by the [Use of eMail and Directory Messaging System Policy](#) and the [UQ Privacy Policy](#). The Federal SPAM act 2003, effective 10th April, imposes harsh fines for unsolicited commercial electronic messages.
- **Inappropriate Emails:** When sending any emails the university policy with respect to gender, race, sexual harassment, bullying and language use applies. Emails and stored information are subject to the Freedom of Information Act (FOI).
- **Unauthorised Private Business:** UQ facilities should not be used for private business use unless written permission has been received from the Head of the Organisational Unit.

3. EXCEPTIONS

The University understands that exceptions may be required for research and teaching and learning purposes. There may also, for example, be instances where P2P functionality is required. In these instances, approval is required from the Head of an organisational unit as legitimate use and notification is to be given to the Director, ITS, who will maintain a register of approved systems.

4. PRIVACY AND MONITORING

The University of Queensland cooperates with network providers, legal authorities of the State and Commonwealth, and the international community to provide a reliable and trustworthy service. Whilst UQ respects the privacy of individuals using UQ facilities, UQ reserves the right to monitor user activity and take appropriate action if misuse of resources is identified.

5. REMOVAL OF MATERIAL

The University has the right to remove, or prevent access to, any information or materials that it deems to be offensive or inappropriate regardless of whether the content is unlawful. Internet sites may be removed without notice.

UQ GUIDELINES IN THE USE OF UQ ICT RESOURCES

VERSION: 1 APPROVAL DATE: 22ND JUNE 2004 . ITSPP

SCOPE: UQ WIDE

PAGE 3 OF 4

Where misuse is identified, or a risk to the security of the network, the Director ITS, or nominee may disconnect systems from the network and machines may be taken into evidence. Where possible and as appropriate, ITS will coordinate with local IT staff and/or the Head of the Organisational Unit.

Depending on the nature of the alleged offence the Director, ITS may advise and seek the advice or assistance of the Secretary and Registrar, Personal Services, Legal Office, Internal Audit, and law enforcement agencies.

6. LIMITED PERSONAL USE

Authorised users are provided with and may use University resources for the purpose of undertaking the duties of their employment by the University (legitimate University purpose). The use of such resources for personal purposes is not generally permitted unless such use is kept to a minimum. Such a minimal use policy is considered appropriate for the personal use of email, the Internet and other University resources.

Limited personal use is defined as:

- Use incurs minimal additional expense to the University
- Use is infrequent and brief
- Use does not interfere with the operations of the University
- Use does not violate any University policy or related State/Federal legislation and regulation.

(State Government Information Standard 38: Use of Communication and Information Devices)

The reasons for limiting personal use are that each and every use of such resources incurs a "cost" to the University and any use which is not a University purpose represents a potential misuse of University resources. Individual personal use may result in relatively small costs being incurred. Continued use or collective use across the University however, may incur many thousands of dollars of costs to the University per annum, money that would be better spent enhancing the level of services currently provided.

Specific Use	Cost to the OU	Cost for 1 hour per person per day for 1mth
Listening to the radio via the Internet	\$1.08 per hour (based on 30Kbps continuous stream)	\$32.76
Watching sporting events eg Olympics	uses a 384kbit stream, \$13.80 per hour.	\$276
Accessing/trading on the stock market	\$1.20 per hour (based on 60 x 200KB pages per hour)	\$36.40
downloading a set of Redhat Linux ISO's	3 x ~625MB	\$131.25
downloading a CD worth (700MB) of video or music (illegal?)	\$49.00	\$49 per CD
Downloading software for personal use	\$70.00/\$99.00 per GB	
Games (assuming multiplayer internet)	\$1.04 per hour (based on 28.8Kbps continuous stream)	\$31.55
Conducting a personal business	\$1.20 per hour (based on 60 x 200KB pages per hour)	\$36.40
Entering non-work related Chat room	\$0.35 per hour (based on 9.6Kbps stream)	\$10.62
Browsing/accessing inappropriate Internet sites	\$1.20 per hour (based on 60 x 200KB pages per hour)	\$36.40
Internet banking and or bill paying	\$1.20 per hour (based on 60 x 200KB pages per hour)	\$36.40
These are all "examples", and the parameters of each can vary significantly, as such costs are indicative only of the charges that may apply. Costs provided by ITS – Network Services 2002.		
This list is not exhaustive but does contain the more common personal use practices.		

7. REPERCUSSIONS FOR NOT ADHERING TO UQ POLICIES

Refer to the Internet Code of Practice for actions that can be taken for inappropriate use.

Where UQ staff and students do not comply with University Policy, misconduct procedures may be instigated. Where breaches of the UQ policies may be inadvertent then a warning from management may suffice. However, where the action has been deliberate and/or there is sustained misuse, then it may be appropriate for management to initiate misconduct procedures. Should the alleged misuse involve an illegal act then the University may be required to report the matter to law enforcement agencies and instigate official misconduct proceedings.

In the event of excessive private use, the University reserves the right to seek recompense for charges incurred from the staff member concerned.

8. INFORMING AND DETECTION OF INAPPROPRIATE USE OF IT RESOURCES

AWARENESS

- Managers should ensure that their staff are aware of the Internet Code or Practice and related guidelines.

STAFF EXTERNAL TO ITS AND STUDENTS

- Where a staff member identifies misuse of UQ resources, they should report this to the manager of the person allegedly responsible for misuse. The manager should take appropriate action depending on the severity of the issue. Action could range from talking to the staff member identified to reporting the issue to the Head of their Organisational Unit who may decide to direct the issue to the Secretary and Registrar. The Director, ITS or nominee are available to provide advice.

9. RELEVANT UQ POLICIES

The following policies are relevant with respect the use of UQ resources

- [HUPP 6.10.1 Internet Code of Practice](#)
- [HUPP 1.50.1 Code of Conduct](#)
- [HUPP 1.50.5 Use of University Facilities](#)
- [HUPP 6.10.4 Information Technology Security Management Policy](#)
- [Use of eMail and Directory Messaging System](#)
- [Email for Staff and Students](#)
- [UQ Privacy Policy http://www.uq.edu.au/privacy/.](http://www.uq.edu.au/privacy/)

This guideline is intended to operate within and be consistent with existing University policies and statutes in areas such as:

- [Management of Sexual Harassment Grievances](#)
- [Discrimination, Harassment and Bullying](#)
- [Racism](#)
- [Freedom of Information](#)
- [Code of Conduct](#)
- [Student Charter](#)
- [Postgraduate Research Student Charter](#) and
- [University of Queensland Statute No.4 \(Student Discipline and Misconduct\) 1999.](#)

10. REVISION HISTORY

VERSION	DATE	EDITOR	SUMMARY OF CHANGES
1 approved	22.6.2004	ITSPP	Approved