University of Wollongong

Information Technology Services

IT ACCEPTABLE USE POLICY

<table>
<tr><td><b>Date approved:</b></td><td>1 July 2004</td><td><b>Date Policy will take effect:</b></td><td>On approval</td><td><b>Date of Next Review:</b></td><td>15 November 2009</td></tr>
<tr><td><b>Approved by:</b></td><td colspan="5">Vice Chancellor</td></tr>
<tr><td><b>Custodian title & e-mail address:</b></td><td colspan="5">Senior Manager Business Services Unit, ITS
michele@uow.edu.au</td></tr>
<tr><td><b>Author:</b></td><td colspan="5">Michele Grange</td></tr>
<tr><td><b>Responsible Faculty/
Division & Unit:</b></td><td colspan="5">Business Services Unit, Information Technology Services</td></tr>
<tr><td><b>Supporting documents, procedures & forms of this policy:</b></td><td colspan="5">Requirements Governing Use of IT Facilities (Annexure 1)
ITS User Guides
University Privacy Statement
EED Unit (Policies, Programs, Training)</td></tr>
<tr><td><b>References & Legislation:</b></td><td colspan="5">Crimes Act, 1914 (Commonwealth)
Student Conduct Rules
Secondary Employment Policy
IT User Account Management Policy
IT Security Policy
Internet Access Policy
Email Access Policy
Telephone Policy
Mobile Telephone Policy
Music, Video and Software Piracy Policy
Web Proxy Authentication Policy</td></tr>
<tr><td><b>Audience:</b></td><td colspan="5">Public – accessible to anyone</td></tr>
<tr><td><b>Expiry Date of Policy:</b></td><td colspan="5">Not applicable</td></tr>
</table>

Contents

1 Purpose of Policy

1. The University of Wollongong is committed to the appropriate use of Information Technology and Services in support of its teaching, research, administrative, and service functions. This policy defines the acceptable behaviour expected of users and intending users of the facilities.

2. Requirements Governing the Use of IT Facilities have been developed in conjunction with this policy. Users of the Information Technology facilities must comply with these requirements which have been designed to allow all users to make optimal and legitimate use of the facilities. The University requires users to accept the IT policies and associated Requirements Governing the Use of IT Facilities (see Annexure 1) as a condition of their use.

2 Definitions

Word/Term	Definition (with examples if required)
University	University of Wollongong
User	Any person using any of the University's Information Technology Facilities
IT facilities	Information Technology facilities operated by the University, whether owned or leased
Chief Technology Officer	The Chief Technology Officer, Information Technology Services
ITS	Information Technology Services at the University of Wollongong

3 Application & Scope

1. This policy and the associated requirements apply to all usage of the IT Facilities. The policy covers computing and communications facilities including telephones, facsimiles, mobile telephones, desktops, printers, photocopiers, email, Internet, web services and similar resources. Usage of remote systems accessed via University IT facilities is covered by this policy and its associated requirements, in addition to any local regulations pertaining to the remote system. This policy represents the University Institutional position and takes precedence over other relevant policies which may be developed at a local level.

2. This policy is consistent with the requirements of academic freedom as defined in the academic staff enterprise agreement.

3. All users should be aware of the policy, their responsibilities and legal obligations. All users are required to comply with the policy and are bound by law to observe applicable statutory legislation.

4 Policy Principles

4. The University of Wollongong IT facilities are provided to assist staff, students and other authorised users to conduct bona fide academic and administrative pursuits.

5. All users must accept full responsibility for using the University's IT facilities in an honest, ethical and legal manner and with regard to the privacy, rights and sensitivities of other people. Use must be in accordance with University policies and all relevant federal and state legislation. Such legislation shall include, but not be limited to legislation covering privacy, copyright, freedom of information, equal employment opportunity, intellectual property and occupational health and safety.

6. ITS provides comprehensive documentation and userguides on the IT infrastructure, services and support. These are accessible at http://www.uow.edu.au/its/userguides/.

7. Staff members are referred to the University of Wollongong Internal Audit (http://staff.uow.edu.au/audit) for information on their role in relation to fraud and corruption prevention.

8. Staff members should be aware of their obligations as to the acceptable use of University Facilities, including IT facilities, in the course of secondary or other employment as outlined in the University's Secondary Employment Policy located in the University Policy Directory.

9. The following general principles apply to usage of IT facilities:

   9.1. An authorised user of the University IT facilities has an assigned user account, which is identified by a username. More detailed information on user accounts is available in the IT User Account Management Policy accessible in the University Policy Directory.

   9.2. Authorised users only may use the facilities and a user may only use those IT facilities to which they are authorised.

   9.3. A user may be given access to a range of IT facilities and is to use these facilities in a manner, which is ethical, lawful, effective and efficient. A user may only use those facilities they have been authorised to use.

   9.4. Where access to a facility is protected by an authentication method, e.g. a password, a user must not make this available to any other person. Users who do so will be held responsible for all activities originating from that account. A user must not use an account set up for another user nor make any attempts to find out the password of a facility they are not entitled to use. A user can expect that access to their account shall not be available to another user. A user must not attempt to find out the authentication secret of any other user.

   9.5. The above does not apply where a user provides access to their account to an authorised support person.

   9.6. The University discourages the storing of passwords due to the security risks this poses.

   9.7. Each user, while using their account, is responsible for:

      a. all activities which originate from their account;

      b. all information sent from, intentionally requested, solicited or viewed from their account;

      c. publicly accessible information placed on a computer using their account.

   9.8. A user must:

      a. show restraint in the consumption of resources;

      b. apply academic and professional integrity;

      c. respect intellectual property and the ownership of data and software;

      d. respect other's rights to privacy and freedom from intimidation, harassment and annoyance;

      e. abide by the University's policies regarding privacy which are accessible at http://www.uow.edu.au/about/privacy/

      f. abide by the University's policies regarding antidiscrimination and harassment accessible at http://staff.uow.edu.au/eed/

   9.9. No user shall:

      a. attempt to subvert the security of any of the University's IT facilities;

      b. attempt to create or install any form of malicious software (for example worms, viruses, sniffers) which may affect computing or network equipment, software or data;

      c. attempt to interfere with the operation of any of the University's IT facilities;

      d. attempt to subvert any restriction or accounting control of any of the University's IT facilities (for example peer-to-peer, web authenticated proxy);

      e. attempt unauthorised access to any University IT facilities.

      f. The above may not apply to authorised support staff in performance of their duties.

9.10. The University network and IT facilities, including email and web servers and other similar resources, may not be used for:

a. the creation or transmission (other than for properly supervised and lawful teaching or research purposes) of any material or data which could reasonably be deemed offensive, obscene or indecent;

b. the creation or transmission of material which the average person deems likely to harass, intimidate, harm or distress;

c. the creation or transmission of defamatory material;

d. the transmission of material that infringes the copyright of another person;

e. the unauthorised transmission of material which is labelled confidential or commercial in confidence;

f. the transmission of any material that contravenes any relevant federal or state legislation;

g. the deliberate unauthorised access to facilities or services.

9.11. No user shall use the University IT facilities for private gain or for financial gain to a third party.

5 Privacy

1. The University seeks to comply with privacy requirements and confidentiality in the provision of all IT Services, but privacy and confidentiality cannot be assured. Users must know that the security of data and networks is not inviolable – most people respect the security and privacy protocols, but a determined person can breach them. Users must also be aware that, network and systems administrators, during the performance of their duties, need to observe the contents of certain data, on storage devices and in transit, to ensure proper functioning of the University's IT facilities.
2. The University's policy and statutory obligations relating to privacy will be upheld in all cases.
3. In addition, any privacy may be subordinate to the application of law or policy, including this policy.
4. Further information on privacy is accessible at http://www.uow.edu.au/about/privacy/

6 Security

1. The University recognises the importance of information technology security and is committed to ensure all business activities performed with the employment of information technology are protected and maintained, and that sustainable procedures are in place to reflect "best practice" information technology security.
2. The University's IT Security Policy is accessible on the University Policy Directory.

7 The Network

1. The University operates a computer network, which is designed to facilitate communication with other universities, or organisations, for students and staff, and other authorised users in support of teaching, research, administrative and service functions.
2. Users should have no expectation of privacy of network traffic although the University will make reasonable attempts to keep traffic private.
3. Users should make every attempt to use secure protocols when accessing network services especially where sensitive or private information is transmitted. This applies particularly to electronic mail.
4. Users should be aware that many protocols transmit authentication details, i.e. username and password, in an insecure manner.

8 The Internet

1. The University encourages the use of the Internet, including email and web services, to facilitate communication among internal users and with the external community; to allow users to better perform the duties assigned to them; and to allow greater efficiency in teaching, research, administrative and service functions.
2. To utilise the University's Internet it is necessary to have a user account. The University's policy on Web Proxy Authentication is accessible on the University Policy Directory.

Internet Access

3. The University's guidelines on internet access and the University's policy on email access are accessible on the University Policy Directory.

9 User Activity

1. When using multi user systems, users should be aware that many of the activities they undertake might be visible to other users. Information which may be available includes session start and end times; origin of session; as well as commands executed and their arguments.
2. Users must also be aware that systems logs of user activity are kept for troubleshooting and accounting purposes. These logs may include times of sent and received mail; email addresses (both sender and recipient), web sites visited and size and type of pages downloaded, files read or written; and machines accessed for any type of network service.
3. The University retains the right to use this information for summary reporting purposes.

10 Telephones and Mobile Telephones

1. The University's policies on telephones and mobile telephones are accessible on the University Policy Directory.
2. Depending on the current load on the University's telephone system local calls may fall to a digital line. As a consequence local calls may be charged as a timed local call. Calls should be made on the assumption that this is the case.

11 Software and Electronic Materials

1. Users are responsible for making use of software and electronic materials in accordance with the Copyright Act, 1968 (Commonwealth), software licensing agreements, and any applicable University policies.
2. Unauthorised copying or communication of copyright protected material (such as music, videos and software), violates the law and is contrary to the University's standards of conduct and business practices. Further information on the University's policy regarding Music, Video and Software Piracy is accessible on the University Policy Directory.

12 Data

1. A user must not examine, disclose, copy, rename, delete or modify data without the express or implied permission of its owner. This includes data on storage devices and data in transit through a network.
2. A user must respect the privacy and confidentiality of data stored or transmitted on the University's IT facilities. Any release of data to those not authorised to receive it is expressly forbidden.
3. Users storing data of a sensitive nature, such as information on individuals whether for academic, administrative or services use must ensure that the privacy of such information is not compromised. In such cases access controls, such as database authentication and encryption, should be employed.

4. In cases where the computer system being used supports file ownership and enforces file access control, files owned by a user should not be accessible to other users. However, in cases where the system supports access control, it is the user's responsibilities to ensure their files have appropriate access control settings to ensure the desired level of privacy and integrity. Wherever possible, systems shall be configured so that the default file permissions on user files will ensure that only the owner of the file can access the contents.

5. The University has a legitimate right to capture and inspect any data stored or transmitted on the University's IT facilities (regardless of data ownership), when investigating system problems or potential security violations, and to maintain system security and integrity, and prevent, detect or minimise unacceptable behaviour on that facility. Such data will not be released to persons within or outside of the University, except in response to:

   a. permission from the user; or

   b. a request from the Senior Executive, Dean, Director or University Librarian, made in writing and accepted by the Chief Technology Officer or delegated persons, to investigate a potential breach of policy; or

   c. a request from the Senior Executive, Dean, Director or University Librarian, made in writing and accepted by the Chief Technology Officer or delegated persons, for access to be granted; or

   d. where deemed appropriate by the University in order to uphold the statutory rights of individuals in matters such as privacy, copyright, occupational health and safety, equal employment opportunity, harassment and discrimination; or

   e. a proper request from an appropriate law-enforcement officer investigating an apparently illegal act, including a court order; or

   f. a relevant statute.

6. Access to any data will always be via network or systems administrators, or via persons nominated by the Chief Technology Officer. The University's policy and statutory legislation relating to privacy will be upheld in all cases.

13 Equipment

1. Users must take due care when using IT equipment and take reasonable steps to ensure that no damage is caused to IT equipment.

2. Users must not use equipment if they have reason to believe it is dangerous to themselves or others to do so.

3. Users must report any damage to IT equipment to appropriate personnel.

4. No user shall without proper authorisation:

   a. attach any device to University IT facilities;

   b. connect any equipment to the University network (for example a modem) that will extend access or provide off-campus access to University IT resources without the prior written approval of the Chief Technology Officer or delegated persons, that such connection meets university security standards;

   c. tamper with or move installed IT facilities without authorisation.

14 Computer Laboratories

1. A user of a computer laboratory shall abide by any instruction or signage as provided by authorised personnel and shall provide relevant identification on request.

2. This policy and the Requirements Governing the Use of IT Facilities apply without exception; however the University reserves the right to apply additional policy and rules specific to individual laboratories.

15 Non-University Use of IT Facilities

1. The University of Wollongong IT Facilities including telephones, facsimiles, mobile telephones, desktops, printers, photocopiers, email, Internet, web services and similar resources are acquired, installed and commissioned for the University's teaching, research, administrative and services purposes. Use for incidental personal purposes (non-University use) may occur but only if that use does not:
    a. interfere with University operation of Information technology;
    b. interfere with other users access to facilities;
    c. burden the University with additional costs; or
    d. interfere with the user's employment or other obligations to the University; or
    e. constitute an offence under any relevant legislation.
2. Where a supervisor considers misuse to have occurred, and such misuse persists after appropriate warning, restrictions may be applied or discipline may be taken under the University's discipline procedures.

16 Administration and Implementation

Compliance

1. The University treats misuse of its IT facilities seriously. Violations of the conditions of use of IT facilities may result in temporary or indefinite withdrawal of access, disciplinary action under the University's or relevant entities discipline procedures, and/or reimbursement to the University.
2. IT misconduct by students will be dealt with under the Student Conduct Rules. The Chief Technology Officer or their nominee will be the Primary Investigation Officer of allegations of IT misconduct by students. Detailed investigation procedures and the penalties that may be awarded to students engaging in IT misconduct can be found in the Student Conduct Rules.
3. A user's access will be withdrawn given a written request from an appropriate staff member of the sponsoring organisation. Access may also be withdrawn by ITS in response to a suspected policy violation.
4. A student whose IT access has been withdrawn as a result of an investigation under the Student Conduct Rules can appeal the decision or the penalty to the Student Conduct Committee. Otherwise, a user whose access has been withdrawn may request reconsideration of the decision by the Chief Technology Officer who shall consider the withdrawal with the relevant Senior Executive, Dean or Director or the University Librarian. Following this the Chief Technology Officer shall confirm the withdrawal or reinstate access.
5. Misuse or unauthorised use of University IT facilities may constitute an offence under the Crimes Act, 1914 (Commonwealth) and/or other pieces of State or Commonwealth legislation. Nothing in this policy or the Requirements Governing the Use of IT Facilities may be taken as in any way diminishing or removing a person's obligations to comply with the law, or their liability to prosecution and punishment under law.
6. Users are encouraged to report any misuse and any reports will be treated as confidential.

17 Roles and Responsibilities

Not Available.

18 Version Control and Change History

Version Control	Date Effective	Approved By	Amendment
1	1 July 2004	Vice Chancellor	Policy converted into new ITS policy format.

			Addition of point re subverting restriction or accounting controls in Section 4 (point 8) Revised compliance statement to conform to the new Rules for Student Conduct. Compliance section under Administration and Implementation changed to include a reference to reimbursement to the University. Improved links to other policies Revised software and electronic materials section inline with the new Music, Video and Software Piracy Policy. Completed the “Rules Governing the Use of IT Facilities” as an appendix to this policy. These are an extraction of the adopted IT policies and replace the now obsolete “Rules governing the use of University computer facilities”. Removed appendix for email etiquette and rules governing the use of computer laboratories from this document.
3	1 September 2004	Vice Chancellor	ITPAC and IT Forum approved version
4	15 November 2005	Vice Chancellor	Included p2p example under General Principles Point 8.
5	6 May 2009	Vice Principal (Administration)	Migrated to UOW Policy Template as per Policy Directory Refresh Renamed the Rules Governing the Use of It Facilities as “Requirements Governing the Use of IT Facilities.”

Annexure 1 – Requirements Governing the Use of IT Facilities

1. Only authorised users may use the IT facilities and a user may only use those facilities to which they are authorised.
2. All users must accept full responsibility for using the University's IT facilities in an honest, ethical and legal manner and with regard to the privacy, rights and sensitivities of other people. Use must be in accordance with University policies and all relevant federal and state legislation.
3. Where access to a facility is protected by an authentication method, e.g. a password, a user must not make this available to any other person. Users who do so will be held responsible for all activities originating from that account. A user must not use an account set up for another user nor make any attempts to find out the password of a facility they are not entitled to use. A user can expect that access to their account shall not be available to another user. A user must not attempt to find out the authentication secret of any other user. The above does not apply where a user provides access to their account to an authorised support person. The University discourages the storing of passwords due to the security risks this poses.
4. Each user, while using their account, is responsible for:
    a. all activities which originate from their account;
    b. all information sent from, intentionally requested, solicited or viewed from their account;
    c. publicly accessible information placed on a computer using their account.
5. University IT policy requires that users:
    a. show restraint in the consumption of resources;
    b. apply academic and professional integrity;
    c. respect intellectual property and the ownership of data and software;
    d. respect other's rights to privacy and freedom from intimidation, harassment and annoyance;
    e. abide by the University's policies regarding privacy;
    f. abide by the University's policies regarding anti-discrimination and harassment;
    g. shall not attempt to subvert the security of any of the University's IT facilities;
    h. shall not attempt to create or install any form of malicious software (for example worms, viruses, sniffers) which may affect computing or network equipment, software or data;
    i. shall not attempt to interfere with the operation of any of the University's IT facilities;
    j. shall not attempt to subvert any restriction or accounting control of any of the University's IT facilities;
    k. shall not attempt unauthorised access to any University IT facilities;
    l. shall not use the University IT facilities for private gain or for financial gain to a third party;
6. The University network and IT facilities, including email and web servers and other similar resources, may not be used for:
    a. the creation or transmission (other than for properly supervised and lawful teaching or research purposes) of any material or data which could reasonably be deemed offensive, obscene or indecent;
    b. the creation or transmission of material which the average person deems likely to harass, intimidate, harm or distress;
    c. the creation or transmission of defamatory material;
    d. the transmission of material that infringes the copyright of another person;

   e. the unauthorised transmission of material which is labelled confidential or commercial in confidence;

   f. the transmission of any material that contravenes any relevant federal or state legislation;

   g. the deliberate unauthorised access to facilities or services.

7. Users are responsible for making use of software and electronic materials in accordance with the Copyright Act, 1968 (Commonwealth), software licensing agreements, and any applicable University policies.

8. A user must not examine, disclose, copy, rename, delete or modify data without the express or implied permission of its owner. This includes data stored on storage devices and data in transit through a network. A user must respect the privacy and confidentiality of data stored or transmitted on the University's IT facilities. Any release of data to those not authorised to receive it is expressly forbidden.

9. Users must take due care when using IT equipment and take reasonable steps to ensure that no damage is caused to IT equipment. Users must not use equipment if they have reason to believe it is dangerous to themselves or others to do so and must report any damage to IT equipment to appropriate personnel. No user shall without proper authorisation:

   a. attach any device to University IT facilities;

   b. connect any equipment to the University network (for example a modem) that will extend access or provide off-campus access to University IT resources without the prior written approval of the Chief Technology Officer or delegated persons, that such connection meets University security standards;

   c. tamper with or move installed IT facilities without authorisation.

10. A user of a computer laboratory shall abide by any instruction or signage as provided by authorised personnel and shall provide relevant identification on request. The University reserves the right to apply additional policy and rules specific to individual laboratories.