

Acceptable Use Policy

Computing and network resources are provided for the use of School of Computer, Electrical and Computer Engineering (SECTE) students and staff in support of teaching and research. All users are responsible for ensuring that they use these resources in an effective, ethical and lawful manner.

1. Scope

This document describes the acceptable use of information technology and applies to all School users of IT resources.

2. Definitions

University is the University of Wollongong

School is the School of Information Technology and Computer Science

IT resource refers to:

all University network services, computer equipment and software owned, leased or used under licence by the University.

IT resources maintained by other bodies but available for use through an agreement or agreements with the University.

External IT resources accessed with University resources

authorised user is any student or staff member of the School or any person officially engaged to undertake School business who uses University IT resources in their role.

user is authorised user.

account is an access control mechanism to identify and authenticate an individual. This commonly takes the form of a username and password. An account may have associated with it access to resources such as access to equipment or file storage.

3. Responsibilities of Users

3.1 Compliance with Laws and Policies

Users must observe all applicable policies and law governing the use of IT resources regardless of location where access is by means of University IT resources. University policies can be found at <http://www.uow.edu.au/its> or copies can be obtained from ITS.

3.2. User Accounts

Accounts are normally established only for individuals. Accounts established for individuals are for their use only. Users shall not use or access any other users account with the exception of authorised University IT support staff while undertaking their duties.

Users must ensure that the authentication mechanism to their account remains secret and is effective. Non-guessable passwords should be used and passwords shall not be disclosed to any person except at the discretion of the user as described below.

Users shall not request access to the secret authentication mechanism for any persons individual account except where an University IT support person requires access to a persons account to perform their duties and other means of access are not reasonably possible. Where an authorised University IT support person requests a users secret account authentication details it may be provided by the user at their discretion.

Users are responsible for any activity carried out using their accounts.

Accounts are to be used solely for those purposes authorised by the University. The user is responsible for the proper use of the account including following recommended procedure for password protection. Access to information is provided on a confidential basis and that confidentiality is to be respected. Where access to IT resources is provided without a formal account and/or password the provisions of these rules still apply.

3.3. Confidentiality of Data

Due to technical limitations, software bugs, system failures and human nature data confidentiality cannot be guaranteed. Network data transmissions may not be secure. Sensitive or confidential material should be encrypted or sent by an

alternative method. E-mail should be viewed as equivalent to mailing a postcard rather than a sealed envelope.

Users should be aware other policies apply in relation to privacy.

3.4. Copyright

Users shall be aware of and comply with any copyright and licensing conditions of data including software stored or transmitted on IT resources.

Specifically, users shall not use any IT resource to violate the terms of any software license agreement or copyright provisions. For example, users shall not copy, disclose or transfer any commercial software provided by the University.

3.5. Personal Identification

Users must show identification including University affiliation upon request to authorised University staff.

4. Acceptable Use

4.1 Use of systems

Other than specifically designated public services, the use of all IT resources is restricted to University users.

University IT resources shall be used for their intended authorised purposes. Incidental personal use is allowable.

A user may not use any IT resource for the purpose of profit-making or commercial activity unless written permission has been obtained from the IT Director or a nominee.

4.2. Threats and harassment

Users shall not use IT resources to harass others or to interfere with their work. For example to send or publish obscene, abusive, fraudulent, threatening, repetitive, chain style or advertising (SPAM) messages to a user or users is a breach of this policy.

Users shall not attempt to deny or interfere with service to other users by means of, for example, "resource hogging", distribution of computer worms, viruses or mail bombing.

4.3. Security

Users shall not attempt to modify IT resources, illegally obtain extra resources, degrade the performance of any system or attempt to subvert the restrictions associated with any computer system, computer account, network service or software protection.

Users shall not attempt to repair or alter the operation of any IT equipment. Faults should be reported to School Technical Support in the first instance or to staff or to ITS.

4.4 Services

Users shall not supply services via the network except with the permission of the Head of School or nominee. Adherence to the Device Security Policy is required when running services.

4.4. Concealed Identity

Users shall not attempt to conceal their identity or masquerade as another person when using IT Resources.

4.5. Data Access

Users shall only access, modify or remove data stored on IT resources for which they have authority to do so.

4.5.1 Data Access by authorised IT personnel

Authorised IT personnel require access to data files and accounts under the following circumstances:

To make backups for the purpose of data loss recovery.

With the permission of the user.

To diagnose system problems or to investigate suspected violations of this policy.

Records will be maintained in cases where action is taken against a user.

Authorised IT personnel should maintain a professional and ethical approach to their work. The SAGE-AU (System Administrators Guild of Australia) Code of Ethics is an appropriate guide.

4.6. University mail lists

Unless the sender is aware of the exact recipients of a mail list (ie lists with small numbers of members) all mail to lists shall:

- be confined to the body of the message (ie no attachments)

- be short (ie less than 100 lines)

- be relevant to the purposes of the list

In addition users shall comply with usage rules specific to certain lists. Specifically, the all staff lists shall only be used for broadcasting information such as:

- Urgent problems with communication services or utilities

- Changes to pre-announced schedule or notification of an important event to occur within the following 24 hours

- University related issues of significance to the majority of University staff.

4.7. Policy Violations

System administrators are authorised to apply certain penalties to enforce applicable policies. Such penalties may include temporary or permanent reduction or elimination of access privileges. This may apply to computing accounts, networks, computing rooms, and other services or facilities.

A user accused of a violation will be notified of the charge and have an opportunity to respond before a final determination of a penalty. If a penalty is imposed, the user may request a review by the Head of School.

If in the opinion of the System Administrator the violation warrants action beyond a System Administrator's authority he or she may refer the case to other authorities such as to the School's disciplinary body appropriate to the violator's status, to an employee's supervisor or to a law enforcement agency.