RULES RELATING TO STUDENT USE OF COMPUTING AND ELECTRONIC COMMUNICATIONS FACILITIES

Responsible Officer	Director of Information Services and Deputy Principal
Contact Officer	Office of the Director of Information Services and Deputy Principal
Superseded Documents	
Review	
File Number	981498
Associated Documents	Student Misconduct Rules

Version	Authorisation	Approval Date	Effective Date
1.0	Authorised by UNSW Council (CL98/70)	28 September 1998	28 September 1998

- Scope
- Rules
  - Definitions
  - Legal Framework
  - Access
  - Non-permitted Use
  - Copyright and Licences
  - Security
  - Related Documents
  - Breaches
  - Schedule of Fines

Scope

UNSW policy is to facilitate the use of information resources by the provision of appropriate and timely technology solutions and technical assistance, and a key strategy of the UNSW Corporate plan is to use information technology in support of the educational, research and administrative activities of the University.

Making information technology more readily available contributes significantly to improving academic quality and student access.

While at UNSW, students are responsible for ensuring that their use of computing and communications facilities is ethical and lawful. They are responsible for ensuring that their actions are not detrimental to the property of the University and the rights of others.

The following rules, which have been made by Council under the University's Student Misconduct Rules, apply across all UNSW facilities. In certain local systems, additional restrictions may apply. The manager of those local resources will advise these additional restrictions.

These rules apply to all student use of University computing or communications facilities. By using any of these facilities, the student is acknowledging that they have read and will abide by these rules. Breach of any of these rules may be considered student misconduct (see Student Misconduct Rules, Section 2.6).

Rules

1. Definitions

1.1 "account" refers to any computing or electronic communication resource allocated for sole or shared usage by a student and protected from general usage by a security system. Such a resource might include, but is not limited to, storage space; access to a computer terminal; processor time; printed output or dial-up access time. A security system might include, but is not limited to, password protection.

1.2 "communications" refers to the use of any of the University's computing and/or electronic communications facilities, including, but not limited to, the University Wide Network, the modem pool, telecommunications, PABX and facsimile equipment to access or transmit information.

1.3 "computing facilities" refers to:

i. all networked services and computer hardware and software, owned, leased or used under licence by the University including the University's academic and administrative systems;
ii. computing facilities maintained by other bodies but available for use through an agreement or agreements with UNSW; and
iii. all other computing facilities, wherever situated, where access is by means of UNSW-provided services.

1.4 "University" means the University of New South Wales.

1.5 "user" means any person or persons utilising, accessing or attempting to gain access to the computing or communications facilities at UNSW.

Any reference to the singular includes a reference to the plural and vice-versa in these rules.

2. Legal framework

Users of computing and communications facilities must be aware that use of these facilities is subject to the full range of State and Federal laws that apply to communications and to the use of computers, as well as any other relevant laws. This includes copyright, breach of confidence, defamation, privacy, contempt of court, harassment, vilification and anti-discrimination legislation, the creation of contractual obligations, and criminal laws.

3. Access

3.1 Access to the University's computing and communications facilities is available to students for teaching, research and administrative purposes, and for other specifically authorised activities.

3.2 Students are entirely responsible for their own accounts and any actions or materials resulting from any use of their accounts.
3.3 The University reserves the right to withdraw the availability of any computing or communications facility without notice.

3.4 Students may use only those facilities to which they have been given specific access by the University or which have been advertised for general student usage, and to the extent and in the manner that they are authorised to use them.

3.5 Students are not to assist persons who do not normally have access to a resource to obtain such access.

4. Non-permitted uses

The following uses and/or activities are not permitted:

4.1 Any use not related to University teaching, learning and research, unless specifically authorised by the University. If a student is unclear of his/her access for purposes unrelated to University teaching, learning and research, clarification should be sought from the relevant University system manager or student supervisor.

4.2 Any commercial purpose.

4.3 UNSW facilities are not to be used for:

- the deliberate or negligent preparing, storing, displaying of racist, pornographic or other offensive material,
- the deliberate receiving or transmitting of racist, pornographic or other offensive material
- unless it is a requisite component of a course of study and has the approval of the relevant lecturer or supervisor.

4.4 Use of the facilities to harass any person (whether within or outside the University) or interfere with their work. Examples of breaches to this rule could include the sending of obscene, abusive, fraudulent, threatening or repetitive messages, as well as unsolicited non-University work-related e-mail.

4.5 Tampering with other users' accounts in any way, including attempting to thwart the system security, setting password traps, and
any other behaviour designed to interfere with other users' access to the facilities.

4.6 Use of other users' accounts, a false identity or another person's identity to gain access to any aspect of the facilities.

4.7 Allowing or assisting another person to obtain access to resources or information not authorised.

4.8 Smoking, eating or drinking in computer laboratories or while using computing facilities at the University.

4.9 Behaviour that impacts adversely on other users in shared spaces, such as making unreasonable noise.

4.10 Deliberately or negligently interfering with the operation or performance of a system by:

- generating excessive load, use of storage capacity, network traffic, etc
- physically damaging or adjusting the equipment. Any such tampering, vandalism, theft or wilful and/or reckless damage may be referred to the police

- introducing viruses or other software components designed to interfere with the normal operation of a system
- deleting, adding or modifying information relevant to the system's operation
- obtaining extra resources without authorisation
- excessive printing
- creating excessive network links

4.11 Circumventing, or attempting to circumvent security or obtaining or attempting to obtain information that would allow security to be circumvented.

4.12 Using a resource not allocated or accessing material not permitted, whether by breaching security, using another's account or taking advantage of another person's negligence. This includes the use of resources in amounts or to a degree other than authorised.

4.13 Copying, disclosure of, transferring, deleting, examining, renaming, changing or adding to software, data or information belonging to UNSW or another person unless permission has been granted or the software, data or information is clearly intended to be public.

4.14 Activities that impact adversely on the University's reputation.

5. Copyright and licences

Students will not copy, disclose or transfer any computer software on the computing and communications facilities provided by the University in such a way as to breach any right of any person (including copyright) without the express written permission of the appropriate University officer or head of school/unit/centre.

6. Security

6.1 The University wishes to maintain a secure, efficient computing and communications environment. It has the right to examine all computer files and to monitor computer usage to ensure compliance with these rules.

6.2 If necessary, computer processes that are actively causing a problem will be terminated, or access to any files related to a breach of the rules removed.

7. Related Documents

These rules operate together with other relevant policies, rules and guidelines of the University on the use of its facilities and resources. These include:

- Student Misconduct Rules
- Breach of Discipline and Misconduct in Assessment
- E-mail Policy

8. Breaches

Students found in breach of these rules are liable to disciplinary action under these rules and the Student Misconduct Rules. Disciplinary action could result in a

warning, a reprimand, suspension of access to computing facilities, a fine or exclusion from the University for a period.

9. Schedule of Fines

The Director of Information Services and Deputy Principal may impose fines of up to $1,000.
The Schedule of Fines will be reviewed annually and published as a separate schedule.

Document Background

This document was developed in consultation with a working party under the guidance of the Director of Information Services and Deputy Principal (DISDP), Ms Christine Page-Hanify. The School of Computer Science and Engineering, together with the Director, had already developed much of the procedure.

Members of the Working Party were:
Ms Christine Page-Hanify, DISDP and Convenor
Dr Keith Burston, Manager, Communications Unit
Professor Ross Jeffery, School of Information Systems
Dr Gernot Heiser, School of Computer Science and Engineering
Mr Geoff Oakley, Manager, Computing Facilities, Computer Science and Engineering
Mr Neil Brown, Acting Manager, Computing Facilities, Computer Science and Engineering
Mrs Patricia Howard, Manager, Client Services, Library
Ms Kathy Keane, Executive Officer, Student Information and Systems Office
Ms Betsy Marks, Administrative Officer, Policy Coordination, Division of Information Services

The Working Party also consulted extensively with Mr Ken Grime and Mr David Caddies of the University Legal Office and Mr David Madden, President of the Student Guild.

For inquiries and further information, please contact the Office of the Director of Information Services and Deputy Principal on
Ph (02) 9385 2602

Appendix A: History

Version	Authorised by	Approval Date	Effective Date	Sections modified
1.0	UNSW Council (CL98/70)	28 September 1998	28 September 1998	Rescinded UNSW Council CL06/81(ii)ii