



<b>UNSW Policy</b>	
<b>Responsible Officer</b>	Chief Information Officer
<b>Contact Officer</b>	IT Policy and Compliance Officer Ext: 52885 Email: <a href="mailto:j.beatson@unsw.edu.au">j.beatson@unsw.edu.au</a>
<b>Approving Authority</b>	Vice-Chancellor
<b>Date Approved</b>	November 2006
<b>Date Effective</b>	1 March 2007
<b>History</b>	This is a new policy
<b>Review Commencement Date</b>	
<b>Related Policies &amp; Documents</b>	<ul style="list-style-type: none"> <li>• This policy <b>replaces</b> the 1998 policy "Rules Relating to Student Use of Computing and Electronic Communications Facilities"</li> <li>• UNSW Code of Conduct</li> <li>• Student Misconduct Rules</li> </ul>
<b>File Number</b>	

**NOTE: THIS POLICY HAS AN ACCOMPANYING PROCEDURES DOCUMENT which must be read in conjunction with the policy.**

## 1. Preamble

Information and communications technology (ICT) has become of critical importance to the University in the support of academic enquiry and research; teaching and learning; core business activities and communications. In recognition of this, UNSW provides computing, email, internet and communication facilities to its staff and students for the purposes of research, teaching and learning; and to support the administration of the University.

This policy informs users of University ICT resources of their rights and responsibilities; and of the University's requirement that its ICT resources are used in a legal, ethical and responsible manner.

This policy also **applies to the use of information** that may be accessed via the University's ICT resources.

This policy supports [the UNSW Code of Conduct](#), which sets out the general rules of conduct for staff of the University.

While the University upholds the principles of academic freedom, it will not condone deliberate breach of either UNSW policies or external legislative requirements and will cooperate fully with the authorities in any investigations resulting from a breach. Consequences of a breach may include the removal of access rights to the University's ICT resources, disciplinary proceedings; and in the case of serious and deliberate breach, may result in civil or criminal proceedings.

Situations not listed here will inevitably arise, and they should be interpreted according to the spirit of this policy.

## **1.1 Principles**

The following principles express the general intent of this policy:

- 1.2.1 The University will provide access to information and communications technology resources to eligible persons according to need and available resources.
- 1.2.2 The University requires legal, ethical and responsible use of its ICT resources.
- 1.2.3 The University will take every precaution to protect the security and privacy of its users' ICT accounts, but users should be aware that normal operation and maintenance of systems includes backup, logging of activity and monitoring of general usage patterns. In addition, the University may be legally required to provide copies of electronic records/communications under subpoena or other legal orders.
- 1.2.4 The University values and respects the principles of academic freedom and freedom of expression, requiring that these be exercised responsibly.

## **1.2 Disclaimer**

While the University will make every effort to ensure the availability and integrity of its ICT resources, it cannot guarantee that these will *always* be available, and/or free of any defects, including malicious software (eg computer viruses). Users should take this into account when accessing the resources.

## **2. Scope**

This is a University-wide procedure which applies to *all* users of University ICT resources – including (but not limited to) staff, students, contractors, third parties, alumni, associates and honoraries, conjoint appointments and visitors to the University.

The policy also applies to anyone connecting personally-owned equipment (eg. laptops) to the University network.

It is important to acknowledge here the dual role of IT professional staff as both IT system administrators and as staff who are also 'standard ICT users'. This policy will apply to those staff while in their role as 'standard ICT users'.

However, in the course of their professional duties, IT staff may be required to undertake actions which are beyond those permitted in this policy. It is expected that they will do so in the spirit of both the University's Code of Conduct and appropriate professional Codes of Ethics, such as that of the System Administrators Guild of Australia (<http://www.sage-au.org.au/ethics.html> - reproduced here with the kind permission of SAGE-AU)

### 3. Definitions

For purposes of this policy, unless otherwise stated, the following definitions shall apply:

Account	Any computing or electronic communication resource allocated to a user by the University and protected from general usage by a security system (eg. password).
ICT (Information and Communications Technology)	ICT includes technologies such as desktop and laptop computers, PDA's, software, peripherals, telephone equipment (including mobile phones) and connections to the Internet that are intended to fulfil information processing and communications functions.
University ICT Resources	(i) All networks, hardware, software and communication services and devices which are owned, leased or used under licence by the University including the University's academic and administrative systems; and (ii) Computing facilities and information resources maintained by other bodies, but available for use through an agreement or agreements with UNSW.
University Network	UNSW central ITS network and other networks provided by the University. Non-UNSW facilities and equipment (eg personally-owned computers) which are connected to the University network will, for the purposes of this document, be considered to be part of the University network.
User, Authorised User	'User' and 'Authorised User' means and includes all staff, students, clinical and adjunct title holders, alumni and other users who are authorised by the University to access its systems and/or network.

### 4. Policy Statements

#### 4.1 Provision of ICT Resources

##### 4.1.1 Rationale

The University recognises the importance of computing and communication technologies and will provide access to ICT resources for its staff, students and other authorised users, for the purposes of research, teaching, learning and administration.

##### 4.1.2 Implications

The University will provide eligible users with access to the ICT resources required to perform their work, research or studies, according to need and available resources.

## **4.2 Legal, Ethical and Responsible Use of ICT Resources**

### **4.2.1 Rationale**

The University requires all users of its ICT resources to do so in a legal, ethical and responsible manner.

### **4.2.2 Implications**

Users of University ICT resources 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 and UNSW policies. This includes (but is not limited to) copyright, intellectual property, breach of confidence, defamation, privacy, contempt of court, harassment, vilification and anti-discrimination legislation, the creation of contractual obligations, civil and criminal laws. In addition, the University's ICT resources must not be used for unauthorised commercial activities or unauthorised personal gain. Use of its ICT resources must not cause loss of service, or risk loss of reputation to the University. Actions performed using the University's computer and network resources, regardless of any disclaimers that might be made, ultimately reflect on the University community as a whole.

In particular, the University's ICT resources must not be used to copy, download, store or transmit material which infringes copyright, such as music files, movies, videos etc.

Actions performed using University ICT resources must comply with the terms of any licence signed by the University for use of online databases, software programs, online publisher packages etc.

### **4.2.3 Limited Incidental Personal Use**

While UNSW ICT resources are provided for the purposes of teaching, learning, research and university administration, limited incidental personal use is allowed, so long as such use:

- Is lawful and compliant with UNSW policies and external legislation;
- Does not negatively impact upon the user's work performance;
- Does not hinder the work of others or interfere with the normal operations of the network;
- Does not damage the reputation or operations of the University; and
- Does not impose unreasonable or excessive additional costs on the University.

**Examples** of acceptable limited incidental personal use include: an online personal banking transaction; an online airline schedule enquiry or booking.

## **4.3 Security and Privacy**

While the University will take every precaution to protect the security and privacy of its users' ICT accounts, users should be aware that legislative (State Records Act) and other requirements require retention and inspection of some electronic files and communications held on the University's systems.

#### **4.3.1 Rationale**

Network and systems administrators treat the content of electronic communications and data as confidential. However, users must be aware that recordkeeping and normal operation and maintenance of the systems generally requires backup and caching of communications and data; the logging of activity; and monitoring of general usage patterns.

#### **4.3.2 Implications**

Since privacy obligations are often defined by situation and circumstances, the University cannot guarantee absolute privacy to users of its ICT resources. The University may be required to inspect or provide copies of electronic communications under law, or when investigating possible misuse of ICT resources.

Users should be aware that electronic records may be subject to the University's obligation to respond to subpoenas or other legal orders (eg. a request under Freedom of Information legislation). For example, email is considered a document under the Law and can be legally requested as can any other document.

Users who have legitimate access to personal and confidential information must respect the privacy of others and maintain the confidentiality of the information to which they have access.

### **4.4 Academic Freedom and freedom of expression**

#### **4.4.1 Rationale**

The University upholds the principles of academic freedom. It values the diversity of cultures, ideologies and perspectives within its community and is respectful of freedom of expression. The University does not condone censorship, nor does it endorse the inspection of electronic files other than on an exceptional basis (eg. when required by law or when investigating a reported violation).

#### **4.4.2 Implications**

The right to academic enquiry and freedom of expression is tempered by the rights of others, including privacy; freedom from intimidation, discrimination or harassment; protection of intellectual property and copyright and ownership of data and security of information.

The University requires all users of its ICT resources to do so in a legal, ethical and responsible manner, in accordance with this and other UNSW policies and relevant State and Federal legislation.

## **5. Legal & Policy Framework**

Users of University ICT resources 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 and UNSW policies. This includes (but is not limited to) copyright, breach of confidence, defamation, privacy, contempt of court, harassment, vilification and anti-discrimination legislation, the creation of contractual obligations, and civil and criminal laws.

The University does not permit its ICT resources to be used for unauthorised commercial activities, unauthorised private gain or that of others. Academic staff are referred to the University's [Policy on Paid Outside Work by Academic Staff](#) with regard to the use of University resources for private professional practice, and all staff are referred to the University's [Code of Conduct](#).

This policy must be read in conjunction with the Procedures for the Acceptable Use of UNSW ICT Resources.

In addition, users should be aware that some third party applications licensed to the University (eg. some of the large searchable databases available through the Library), have their own Terms and Conditions which may apply over and above this policy.

## **6. Implementation**

### **6.1 Responsibilities**

The Chief Information Officer has the responsibility for coordinating the implementation of this policy and its associated documents.

#### **6.1.1 Compliance and Breaches**

##### **(a) Notifying violations**

Staff and students who become aware of possible violations of this policy should report them immediately to an appropriate person, such as their supervisor, the system administrator, computer lab manager or Head of Department/School. Alleged serious or repeated breaches must be reported to the UNSW Chief Information Officer. In cases where personal safety may be at risk, unauthorised entry to a computing facility has occurred or, where it is believed necessary to seize material held on a University computer, UNSW Security should be contacted for advice and assistance.

##### **(b) External Requests for Information**

If a request is received from an external organisation for information held on University computers (eg. copies of emails or other correspondence) it must be passed immediately to the University's Legal Office for investigation and action.

##### **(c) Penalties associated with violations**

Penalties will depend upon the type and severity of breach. Penalties may range from loss or restriction of access, to formal University disciplinary action for breach of ["Student Misconduct Rules"](#) (students) or ["Code of Conduct"](#) (staff). Cases of serious, deliberate, and/or criminal breach will be referred to external authorities and may result in civil or criminal proceedings.

The University reserves the right to limit access to its networks through University-owned or other computers and to remove or limit access to material and resources stored on University-owned computers.

Formal disciplinary action for students will occur in accordance with "Student Misconduct Rules" and may include financial penalties as determined by the Chief Information Officer (See Procedures Document, Appendix 1).

Formal disciplinary action for staff will occur via the procedures outlined in the current UNSW General and Academic Staff Enterprise Agreements.

### **6.2 Support**

For guidance and advice regarding the implementation of this policy contact the IT Policy and Compliance Officer on ext 52885.

## 7. Evaluation

It is anticipated that this policy will be reviewed 2 years after its implementation date, and every 2 - 3 years thereafter.

## 8. Associated Documents

Appendix 1: Documents referenced in this policy

Procedures for the Acceptable Use of UNSW ICT Resources

## 9. Acknowledgements

Documents referenced in this policy are listed in Appendix 2

## 10. Document History

This policy was developed by Jenny Beatson, IT Policy and Compliance Officer, Information Technology Services (ITS) and a working party consisting of the following members:

• Carol Kirby, Legal Office	• Eryl Brady, Equity and Diversity Office
• Mark Fisher, ITS	• Rob Morell, UNSW Student Services
• Graham Hannah, FBE	• Cecilia White, DVC Resources
• Jim Leeper, Faculty Medicine	• Dawesh Chand, Faculty Law
• Tony Ablong, ADFA	• Sharon Brogan, COFA
• Shawn Sjinstra, FCE	• Geoff Oakley, FacEng
• Ben Low, ITS	• Howard Amos, Library
• Tony Koppi, EDTeC	• Rebecca Edwards, Policy Mgt Unit
• Joe Fenech, AGSM	• Greg Fallon, FASS
• Michael Rourke, ITS	• Tom Sedgwick, Faculty Science

I am grateful to Sharon Brogan for permission to use references from the COFA Staff Computer Use Policy; and to the System Administrators Guild of Australia for permission to reference the SAGE-AU Code of Ethics.

### Document History

Version	Date	Author	Details
0.1	19 Jan 05	J Beatson	First Draft
0.2	18 May 05	J Beatson	After M Fisher feedback
0.3	11 Dec 05	J Beatson	After review by E Brady, C Kirby
0.4	13 Mar 06	J Beatson	Amendments after Workshop 15 Feb
0.5	24 May 06	J. Beatson	Re-format into new UNSW policy template; incorporate additional feedback from w/shop and Legal Office
0.6	26 June 06	J. Beatson	Incorporate further feedback, add SAGE-AU Code of Ethics reference.
0.7	17 July 06	J. Beatson	Amend/edit to incorporate ASC feedback from mtg 11.7.06
0.8	8 Aug 06	J Beatson	ASC feedback from mtg 8/8/06. THIS VERSION TO PUBLIC CONSULTATION.
0.9	25 Sept 06	J. Beatson	Amend/Edit to incorporate feedback from PAC mtg 12/09/06 and feedback from period of public consultation. Submitted to and approved by Academic Board, Oct 3 2006

### Approved:

..... Date: .....

Tim Cope, Chief Information Officer

## ***Appendix 1: Documents Referenced in Developing this Policy***

### ***State and Commonwealth Legislation***

Telecommunications Act, 1997  
Broadcasting Services Act, 1992  
Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Act (No 2), 2004  
Privacy and Personal Information Protection Act 1998 (NSW),  
Privacy Act 1988 (Commonwealth),  
Copyright Act 1968  
Internet Content Codes of Practice – Australian Communications and Media Authority  
Commonwealth Racial Discrimination Act, 1975  
Commonwealth Human Rights and Equal Opportunity Commission Act 1986  
Commonwealth Sex Discrimination Act 1984  
Commonwealth Disability Discrimination Act 1992  
Education Services for Overseas Students Act, 2000 (ESOS)  
Commonwealth Spam Act, 2003  
NSW Crimes Act, 1900 (and subsequent amendments)  
NSW Anti-Discrimination Act, 1977 (and related legislation)  
NSW Occupational Health and Safety Act, 2000  
NSW State Records Act, 1998  
NSW Workplace Surveillance Act, 2005

### ***UNSW Policies***

UNSW Code of Conduct (Staff),  
UNSW Intellectual Property Policy,  
Student Misconduct Rules,  
Responsible Copyright Practices at UNSW  
UNSW Privacy Management Plan,  
UNSW Equity and Diversity Policy Statement  
Staff Discrimination and Harassment Grievance Policy and Procedures  
Student Discrimination and Harassment Grievance Policy and Procedures  
UNSW Guidelines for Commercial Activities  
UNSW Electronic Record-Keeping Policy  
UNSW Record-Keeping Policy  
UNSW IT Security Policy  
UNSW Website Policy  
UNSW Email Policy  
Policy for making a complaint or reporting incidents of criminal, corrupt conduct or Maladministration or Protected Disclosure at UNSW  
UNSW Policy on Paid Outside Work by Academic Staff  
Student Misconduct Rules