# Procedures for the Acceptable Use of UNSW Information and Communication Technology Resources

| | |
|---|---|
| **Policy Hierarchy link** | Acceptable Use of UNSW Information and Communication Technology Resources. |
| **Responsible Officer** | Chief Information Officer |
| **Contact Officer** | IT Policy and Compliance Officer<br>Ext: 52885<br>Email: j.beatson@unsw.edu.au |
| **Superseded Documents** | |
| **File Number** | Contact the Records & Archives Office. |
| **Associated Documents** | UNSW Code of Conduct |

| Version | Authorised by | Approval Date | Effective Date |
|---|---|---|---|
| 1.0 | Vice-Chancellor | November 2006 | 1 March 2007 |



## 1. Purpose

This procedure details the specific actions and process that must be followed to implement the policy on **Acceptable Use of UNSW ICT Resources**. The procedure outlines the responsibilities of all users of UNSW ICT 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, associates and honoraries, alumni, conjoint appointments and visitors to the University.

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

## 3. Definitions

For purposes of this procedure the definitions listed in the policy on **Acceptable Use of UNSW ICT Resources** will apply.

# 4. Actions & Responsibilities

## *4.1 Provision of ICT Resources*

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

Accordingly, access to University ICT facilities is in accordance with need, availability and is subject to the policy on **Acceptable Use of UNSW ICT Resources**.

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

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

### 4.2.1 Respect for Intellectual Property and Copyright

Although the Internet allows easy access to information, images, musical recordings, films, videos, software and other intellectual property, it does not mean these things are therefore freely available to copy or download. Much material is accessible on the Internet without the copyright owner's permission. University ICT resources must not be used to copy, download, store or transmit material which infringes Copyright. Users of University ICT resources are responsible for complying with Copyright law (refer to the UNSW Copyright website)

Users will respect the copyright and intellectual property rights of others, including by:

- Using only appropriately-licensed and authorised computer software programs;
- Complying with the terms of any license signed by UNSW for online databases, software programs, online publisher packages, etc;
- Ensuring copyright material is only copied or used with the permission of the copyright owner, under the terms of a copyright licencing agreement, or as permitted by law.

*Examples of inappropriate use include (but are not limited to):*

- Making/using illegal copies of a licensed computer program;
- Downloading, copying, storing or transmitting material such as music, video or movie files without the express permission of the copyright holder or as permitted by law.
- Downloading unrelated to teaching, learning or research which incurs significant additional cost to the University.

### 4.2.2 Use ICT Resources Efficiently and Professionally

Computing resources are finite and must be shared by many - users should ensure they are efficient and professional in their use of the network facilities, services and applications they are required to use in their positions. Examples of efficient and professional use include:

- Communication of work-related information (e.g. email) is expressed with the same professional care and courtesy as is given to a signed paper memo;

- Users receive appropriate training in the applications they are required to use in their daily work;
- Users ensure that personal incidental use of ICT resources is kept to a reasonable minimum (see Section 4.2.3 of Policy document for examples of acceptable personal incidental use).

*Examples of inappropriate use include (but are not limited to):*

- Downloading large files without permission ("hogging" bandwidth);
- Excessive printing using a shared facility;
- Excessive personal use of ICT resources;
- Eating, drinking or making undue or excessive noise in a shared computing facility (eg a computer laboratory) where this is not permitted.

### 4.2.3 Use ICT Resources in a Legal and Ethical Manner

Use of the University's ICT resources is subject to the full range of State and Federal legislation, as well as UNSW policies. Users need to ensure that their use of ICT resources is legal and ethical at all times.

Examples of unlawful/inappropriate use of University ICT resources include (but are not limited to):

- Create/send email under another's name (forgery);
- Create/send/forward: electronic chain letters, unsolicited broadcast emails ("Spam"), obscene, abusive, fraudulent, threatening or repetitive messages;
- Use of ICT resources to harass, threaten, defame, vilify or discriminate against any group or individual;
- Intentional or irresponsible damage of ICT resources;
- Theft of equipment;
- Connection of a device to the UNSW network which is configured to breach this policy.

It is acknowledged that access to potentially unlawful or inappropriate material may be required for legitimate research and teaching purposes. However, access to the following material remains inappropriate **UNLESS** it has been authorised in writing by a Head of School (or equivalent) as legitimately required for teaching and/or research purposes (including Ethics approval where appropriate) **AND** access to the material is restricted to legitimate users:

a) Access gambling sites or material that is obscene, pornographic, paedophilic, discriminatory or vilificatory, that promotes illegal acts, or that advocates violence;

b) Use of ICT resources to obtain, store, display, copy or transmit *potentially* unlawful or obscene material.

**Under no circumstances** may UNSW ICT resources be used for or in relation to corrupt conduct, unauthorised personal financial or commercial gain, or for the unauthorised financial or commercial gain of a third party. Academic staff are referred to the UNSW "Paid Outside Work" policy and general staff to the UNSW Code of Conduct.

### 4.2.4 Access by Minors

The Broadcasting Services Act (1992) requires Internet Service Providers to obtain permission from parents or guardians before providing a user account to a person under 18 years of age (including University students). At the time of writing, it is not clear whether this requirement is also applicable to Universities, although several have already instigated such a process.

Departments which run outreach programmes for minors which involve internet access (eg bringing high-school students onto campus for study or recruitment purposes) can cover this likelihood by ensuring that the school excursion permission slip includes reference to parent/carer permission to access the internet.

## *4.3 Security and Privacy*

UNSW employs various measures to protect the security of its ICT resources and of its user accounts, as described in the Policy document.

Users will protect computer systems, information and accounts by:

- Choosing “strong” passwords and/or changing passwords periodically (a “strong” password is one that is hard for others to guess - it should contain a mixture of letters and numbers and should not be as simple as a birth-date or pet’s name).
- Keeping their login details confidential - users are responsible for all activities occurring using their accounts;
- Using their access only as authorised;
- Respecting the privacy and confidentiality of information to which they may have access;
- Using and keeping up-to-date recommended anti-virus programs and operating system/security patches;
- Downloading, installing or using only authorised and licensed software programs;
- Promptly reporting any breach or gap in system or network security to their system administrator;
- Performing a virus check on email attachments and disks before opening.

Examples of unacceptable use include (but are not limited to):

- Allowing others to gain unauthorised access using your login and password;
- Passing on private or confidential information to persons not authorised to access that information;
- Gaining unauthorised access to systems by any means, including port scans, ‘hacking’ and use of ‘password sniffer’ software;
- Using UNSW ICT resources to attack or compromise any other system, whether on or off-campus;
- Downloading, installing or using unauthorised/unlicensed software programs;
- Knowingly propagating or installing computer viruses or malicious code;
- Accessing or intercepting others’ electronic communications without permission.

#### 4.3.1 Staff Exit procedures

When an employee leaves the University, supervisors must ensure that all access to UNSW administrative systems, networks, email accounts etc. is removed or amended as appropriate upon the employee's departure from UNSW.

If there is to be a continuing relationship with the University after exit (eg. Honorary appointment, Emeriti, alumnus) then appropriate access to ICT resources can be allocated as per need.

It may be necessary for a supervisor to access work files or email accounts after an employee's departure from the University in order to preserve continuity of work. In these circumstances, a departing employee will normally be given the opportunity to remove any personal files or email from University computers prior to their departure.

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

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

This procedure must be read in conjunction with the policy on **Acceptable Use of UNSW ICT Resources,** which contains a list of relevant policies and legislation.

It should also be noted that student misuse of ICT Resources can be regarded as Academic Misconduct (under the Student Misconduct Rules) and that financial penalties can be imposed by the University's Chief Information Officer.

## 6. Evaluation

This procedures document will be subject to periodic review, both in its own right and when changes occur with other impacting policies and/or legislation.

## 7. Associated Documents

UNSW Policy on Acceptable Use of UNSW ICT Resources.

# Appendix 1: Schedule of Student Fines for Misuse of ICT Resources

Student misuse of ICT resources is regarded as Academic Misconduct under the *Student Misconduct Rules.* The Chief Information Officer (CIO) and the University Librarian have delegated authority from Council to impose fines of up to $1,000 for student misuse of computing facilities. Below are *examples of fines* that may be imposed, depending on the severity of the breach. Repeat breaches may attract larger fines and penalties. The disciplinary and appeals process is as outlined in the *Student Misconduct Rules,* which may be viewed at: http://www.policy.unsw.edu.au/policy/stumis.htm

It should also be noted that serious and/or repeated breaches may result in civil or criminal proceedings.

| Breach | Fine |
|---|---|
| Smoking, eating or drinking in laboratories, or while using computer facilities, unless this is permitted by local policy* | $24 |
| | |
| Sending inappropriate material via email, news broadcasts, Internet Relay Chat or other methods. | $120 |
| | |
| Using computing facilities for unauthorised/private commercial gain. | $240 |
| | |
| Download/install/use peer-to-peer or other file-sharing software unless this is permitted by local policy* | $240 |
| | |
| Excessive downloading, without authorisation, of material unrelated to your course of study. | $240 |
| | |
| Misuse of licensed databases, such as attempting to download more than is permitted by the licence. | $240 |
| | |
| Damage to equipment or interfering with the normal operation of the system. | $240 |
| | |
| Disclosing your password to others or using another's account. | $360 |
| | |
| Breaching security of computing or electronic communications systems belonging to UNSW or others. | $360 |
| | |
| Infringing copyright by uploading/ downloading material such as music, video, movie, or TV programme files without licence agreement or the express permission of the copyright owner. | $480 |
| | |
| Preparing, storing, displaying or sending racist, pornographic, threatening, harassing or other offensive or illegal material. | $480 |
| | |



* Local policy is one initiated and implemented at the local level within a Faculty, School or business unit. These are permitted as long as they do not conflict with UNSW policy.

Schedule approved by the Academic Board June 2007.This schedule will be reviewed every 2 years: next review date June 2009.