Acceptable Use of UNSW Information and Communication Technology (ICT) Resources Procedures

Version	Approved by	Approval date	Effective date	Next review
2.1	Vice-President, Finance and Operations	27 September 2016	27 September 2016	June 2017

Procedure Statement			
Purpose	This procedure supports the *Acceptable Use of UNSW Information and Communication Technology (ICT) Resources Policy*.		
Scope	This is a University-wide procedure which applies to **all** users of University ICT resources – including (but not limited to) staff (including casuals), students, consultants and contractors, third parties, agency staff, alumni, associates and honoraries, conjoint appointments and visitors to the University. This Procedure applies to the use of UNSW ICT and ICT resources. The Procedure also applies to anyone connecting personally-owned equipment (eg. laptops) to the University network.		
Are Local Documents on this subject permitted?	☐ Yes	☐ Yes, subject to any areas specifically restricted within this Document	☐ No
Procedure Processes and Actions			

Contents

1. Provision of ICT Resources

- The University will provide staff, students and other authorised users with access to the ICT resources required to perform their work, research or studies, according to need and available resources.
- Computers and ICT resources are provided for legitimate University activities and all usage must be consistent with this purpose. Limited, incidental personal use is allowed subject to the conditions outlined *below, under the section* ***Limited Incidental Personal Use***.
- 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 (e.g. computer viruses). Users should take this into account when accessing the resources.

2. 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. 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.

2.1. Respect for Intellectual Property and Copyright

i. The Internet allows access to information, images, musical recordings, films, videos, software and other intellectual property, but 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.

ii. 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 licensing 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.

2.2. Use ICT Resources Efficiently and Professionally

i. Computing resources are finite and must be shared by many - users should ensure they are efficient and professional in their use of network facilities, services and applications.

ii. 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 below for examples of acceptable personal incidental use).

iii. 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 (e.g. a computer laboratory) where this is not permitted.

2.3. Use ICT Resources in a Legal and Ethical Manner

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

ii. 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 that is configured to breach this policy.

iii. 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 by Academic Staff* Policy and general staff to the UNSW Code of Conduct.

2.4. Limited Incidental Personal Use

i. 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.
- ✓ Does not impose unreasonable or excessive additional costs on the University.

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

3. Monitoring usage of ICT and ICT Resources

The University takes non-compliance with this set of policy and procedure seriously and if any user breaches the standards of use it may result in the following:

- *Staff:* The University may take disciplinary action in accordance with applicable Enterprise Agreements - in serious cases, this may include termination of employment.
- *Students*: The University may deal with non-compliance in accordance with applicable policies and procedures. This may include the University levying fines against non-complying students or taking other action. In serious cases this may involve expulsion. ***See Appendix 1.***
- Non-staff members may have commensurate action taken against them, which may include termination or non-renewal of their appointment or contract. Use of or access to ICT and ICT resources may also be restricted or removed.

Consistent with these purposes, UNSW will normally only access an employee's records in the following circumstances:

1. When an employee is unexpectedly absent from work (for example, on sick leave or annual leave) and access is required for legitimate business purposes (for example, work continuity) or occupational health and safety reasons (for example, where there are reasonable concerns about the individual's health and safety).

2. When UNSW reasonably suspects that an individual(s) is not complying with this Policy, other UNSW policies or procedures (e.g. Code of Conduct), or legislation.
3. For use in legal proceedings or as required by law (e.g. to comply with a Notice to Produce or subpoena).
4. For IT security purposes (e.g. to protect networks or data stored on the network).

Consistent with this approach, access to an employee's records will only be granted with the approval of the Chief Digital Officer and the Director, Human Resources (or their nominee in circumstances of absence). Access to the records will be provided to an appropriately senior person nominated by the Chief Digital Officer and Director, Human Resources.

Consistent with these purposes, UNSW will normally only access a student's records in the following circumstances:

1. For use in misconduct proceedings in accordance with student, staff or research misconduct procedures where that relates to complying with UNSW policies and procedures.

Consistent with this approach, access to a student's records will only be granted with the approval of the Chief Digital Officer and appropriate Deputy Vice Chancellor (or their nominee in circumstances of absence). Access to the records will be provided to an appropriately senior person nominated by the Chief Digital Officer and Deputy Vice Chancellor.

For more information on the *Workplace Surveillance Act (NSW)*, refer to the UNSW Acceptable Use (ICT) Policy.

3.1. Staff Exiting Procedure

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 (e.g. 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. Academic Freedom and freedom of expression

- The University upholds the principles of academic freedom. This 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.
- While the University upholds the principles of academic freedom, it will not condone breaches of 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.

5. Breaching the conditions of use

- All users must comply with the conditions of use set out in the Policy. If any user breaches the conditions of use in the Policy, the University may take disciplinary action. In serious cases, this may include termination of employment or expulsion from the University. Non-staff members may have commensurate action taken against them, which may include termination or non-renewal of their

appointment or contract. Use of or access to ICT and ICT resources may also be restricted or removed.

- If the University becomes aware of any criminal conduct or an alleged breach of any Australian law, the University may notify the Police or other relevant government authority (e.g. Independent Commission against Corruption).
- For student fines for misuse of ICT resources, refer to ***Appendix 1: Schedule of Student Fines for Misuse of ICT Resources***. The disciplinary and appeals process is outlined in the Student Code Policy and associated *Student Misconduct Procedures.*

6. Implementation

6.1. Responsibilities:

The Chief Digital Officer has the responsibility for coordinating the implementation of this set of policy and procedure.

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 School. Alleged serious or repeated breaches must be reported to the Chief Digital 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 (e.g. 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 (which in serious cases may include termination or expulsion). 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 Procedures and may include financial penalties as determined by the Chief Digital Officer (see Appendix 1).

Formal disciplinary action for staff will occur via the procedures outlined in the relevant industrial instrument (e.g. an applicable enterprise agreement).

Accountabilities	
Responsible Officer	Chief Digital Officer
Contact Officer	Email: itpolicy@unsw.edu.au
Supporting Information	
Parent Document (Policy)	Acceptable Use of UNSW Information and Communication Technology (ICT) Resources Policy.
Supporting Documents	Appendix 1: Schedule of Student Fines for Misuse of ICT Resources

Related Documents	UNSW Code of Conduct UNSW Student Code Policy Student Misconduct Procedure UNSW Research Code of Conduct Procedure for Handling Allegations of Research Misconduct
Superseded Documents	Acceptable Use of UNSW Information and Communication Technology (ICT) Resources Procedure v2.0, approved by the President and Vice-Chancellor on 6 June 2013.
UNSW Statute and / or Regulation	Nil
Relevant State / Federal Legislation	Refer to the Acceptable Use of Information and Communication Technology (ICT) Policy.
File Number	2010/02659

Definitions and Acronyms

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).
University ICT Resources	(i) All networks, hardware, software and communication services and devices which are owned, leased or used under license 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.
ICT (Information and Communications Technology) (Includes both university owned and personally owned equipment)	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 fulfill information processing and communications functions.
University Network	UNSW IT's 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.

Revision History

Version	Approved by	Approval date	Effective date	Sections modified
1.0	Vice-Chancellor	November 2006	1 March 2007	
1.1	Head, Governance Support	18 February 2010	18 February 2010	Section 1, 3, 4.1, 4.2.1, 5, 7, Appendix 1
2.0	President and Vice-Chancellor	6 June 2013	30 June 2013	Full review
2.1	Vice-President, Finance and Operations	27 September 2016	27 September 2016	All sections re-numbered; Section 3 (student records); Section 6 and Appendix 1 (senior position titles)

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 Procedures.* The Chief Digital Officer (CDO) at UNSW and the University Librarian have delegated authority from Council to impose fines and penalties.

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 Procedures.*

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.	$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 Procedures*	$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 Procedure is 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 or Procedure.