



**Acceptable Use of ICT Resources Policy (Students)**

|                                      |   |
|--------------------------------------|---|
| <b>Category/Business Group</b>       | Corporate Services – Information Technology |
| <b>Published Externally (Yes/No)</b> | Yes   |
| <b>Approver</b>                      | Chief Executive Officer                     |
| <b>Responsible Officer</b>           | Head of Information Technology              |
| <b>Contact Officer</b>               | IT Helpdesk Team Leader                     |
| <b>Effective Date</b>                | 1/10/2018                                   |
| <b>Next Review Date</b>              | 1/10/2021                                   |
| <b>Version</b>                       | 1   |

**Policy Approval**

| <b>Approver</b> | <b>Responsible Officer</b> | <b>Policy Officer</b> |
|-----------------|----------------------------|-----------------------|
| Rob Forage      | Simon Paine                | Emma Drummond         |
| Date: 2/10/2018 | Date: 21/09/2018           | Date: 21/09/2018      |

## 1. Background

Information & Communication Technology (ICT) Resources are essential tools for UNSW College in the provision of innovative education programs. In recognition of this, UNSW College provides Students with access to a range of network and computing resources for legitimate learning purposes and communications.

## 2. Purpose

This Policy informs UNSW College Students of their rights and responsibilities in the use of computing and network resources owned or operated by UNSW College and/or UNSW.

This Policy should be read in conjunction with the [UNSW Student Code of Conduct](#), [Acceptable Use of UNSW Information and Communication Technology \(ICT\) Resources Policy](#) and [UNSW College Student Misconduct Policy](#).

## 3. Scope

This Policy applies to UNSW College students who access and use the ICT Resources provided by UNSW College and/or UNSW. Use of these resources includes access from on campus and off campus, as well as access from privately owned computers and electronic devices.

This Policy applies to the use of ICT Resources at all times, regardless of whether such use occurs during business hours. This Policy also applies to the use of information that may be accessed via the ICT Resources.

## 4. Definitions

**Excessive Downloading** means downloading, without authorisation, of large volume contents unrelated to UNSW College Students' course of studies. This includes but is not limited to:

- (a) downloading entire volumes or archives of e-journals, e-books or multimedia resources;
- (b) using robots, spiders, or other automated programs to download entire websites or online repositories; and
- (c) downloading or streaming high definition and/or high-quality video.

**Illegal Content** means content which breaches Australian law and includes but is not limited to:

- (a) child sexual abuse material or child exploitation material;
- (b) material advocating a terrorist-related act; and
- (c) material promoting racism or other forms of discrimination.

**Information & Communication Technology (ICT) Resources** include but are not limited to the following resources provided by UNSW and/or UNSW College:

- (a) online learning systems (e.g. Moodle);
- (b) email accounts (when applicable);
- (c) communication systems;
- (d) network connections (e.g. WiFi);

- (e) Internet and Student Intranet access;
- (f) locations on the network for storage of files (when applicable);
- (g) software applications;
- (h) classroom computers; and
- (i) printers, scanners and copiers.

**Non-Academic Misconduct** means all Student misconduct other than Academic Misconduct, as referred to in the [UNSW College Student Misconduct Policy](#).

**Program** means a course of education or training offered by UNSW College.

**Prohibited Offensive Content** includes:

- (a) depictions of actual sexual activity between adults;
- (b) videos showing very high-impact violence;
- (c) footage detailing offensive sexual practices; and
- (d) material which encourages violence, criminal behaviour, or dangerous behaviour, such as creating weapons, taking or making drugs, or carrying out fraudulent/terrorist acts.

**Spam** means electronic junk mail – unsolicited messages sent by email, text message or instant message without the recipient’s consent.

**UNSW** means the University of New South Wales Sydney.

**UNSW College Students** (hereafter referred to as “**Students**”) means all UNSW College Students, including:

- (a) Students who are enrolled with UNSW College to study a Program which is delivered by UNSW College; and
- (b) Students previously enrolled, not currently enrolled and Students on program leave, where the event forming the basis of the alleged misconduct occurred while they were enrolled, or is directly related to their enrolment.

## 5. Policy Statement

### 5.1. Agreement to be Bound by this Policy

By accessing and using the ICT Resources, Students agree to be bound by the terms outlined in this Policy.

### 5.2. Conditions of Use

- (a) Students using ICT Resources are subject to the full range of applicable laws, including but not limited to: copyright; intellectual property; confidentiality; defamation; privacy; harassment; vilification and anti-discrimination legislation and civil and criminal laws.
- (b) Students agree to protect UNSW College ICT systems, information and accounts by:
  - (i) respecting copyright and intellectual property rights of others;
  - (ii) using access only as authorised;
  - (iii) keeping account details confidential;
  - (iv) using only authorised and licensed software programs; and

- (v) promptly reporting any breach in system or network security to their teacher or to Student Services.

### 5.3. Principles

Consistent with the [UNSW Student Code of Conduct](#) and [UNSW College Student Misconduct Policy](#):

- (a) Students must use ICT Resources with due care and seek advice from their teacher or Student Services if they are in doubt whether a particular use is acceptable or whether they are eligible to use a particular ICT Resource;
- (b) Students must not use ICT Resources in an unauthorised way; and
- (c) Students are permitted limited and reasonable personal use of ICT Resources.

### 5.4. Unacceptable and Unauthorised Uses of ICT Resources

Students must use ICT Resources in a legal, ethical and responsible manner. Students are not permitted to:

- (a) remain logged in on a UNSW College computer after use;
- (b) undertake Excessive Downloading;
- (c) use another's login or password (with or without the owner's consent) or allowing others to use their login or password;
- (d) install any game(s) or other program(s) onto any UNSW College computer(s), or copy any game(s) or other program(s) to UNSW College computers;
- (e) eat, drink, smoke, play loud music or loud computer games in the computer labs;
- (f) make/use illegal copies of a licensed computer program;
- (g) download, copy, store or transmit copyrighted material such as music, graphics, video or movie files without the express permission of the copyright holder or as permitted by law;
- (h) gain unauthorised access to systems by any means, including port scans, 'hacking' and use of 'password sniffer' software;
- (i) use ICT Resources to attack or compromise any other system, whether on or off-campus, including circumventing system security or protection measures;
- (j) knowingly propagate or install computer viruses or malicious code;
- (k) access or intercept others' electronic communications and/or files without permission;
- (l) create or send email under another's name;
- (m) create, send or forward electronic chain letters, Spam, obscene, abusive, fraudulent, threatening or repetitive messages;
- (n) distribute proprietary data or other confidential information such as exam materials, assessment and assignment questions which are the property of UNSW College, in violation of UNSW College policies, procedures or any other written agreements;
- (o) cause intentional or irresponsible damage to ICT Resources, or steal equipment;

- (p) access Illegal Content and Prohibited Offensive Content;
- (q) access gambling sites;
- (r) use ICT Resources for unauthorised commercial activities or for unauthorised personal gain; and
- (s) use ICT Resources in a manner causing loss of service, or risking loss of reputation to UNSW College.

### **5.5. Personal Use of ICT Resources**

- (a) Access to ICT Resources for personal use is permitted within reasonable limits, provided it does not have an adverse impact on:
  - (i) classes and other teachers;
  - (ii) other Students' study;
  - (iii) the availability and/or operation of the resource;
  - (iv) the cost of operating and maintaining the resource;
  - (v) the legal obligations, reputation and standing of UNSW College or of UNSW.
- (b) UNSW College does not accept any responsibility or liability for any damage to, or loss of, personal or work data, hardware or software, arising directly or indirectly from Students' use of ICT Resources for non-study related purposes, or for any consequential loss or damage.

### **5.6. Third Party Applications**

Some third-party applications licensed to UNSW and to UNSW College have their own terms and conditions, which may apply over and above this Policy. Students are expected to comply with these terms and conditions when using such third-party applications.

### **5.7. Privacy, Monitoring & Access**

- (a) UNSW College employs various measures to protect the security and privacy of its ICT Resources, however Students should note that the security of data and networks can be breached.
- (b) Students should also be aware that normal operation and maintenance of ICT Resources includes backup, logging of activity and monitoring of general usage patterns.
- (c) The technology supporting ICT Resources involves recording, backup and monitoring of all usage (including emails, Internet, hard drives and networks) for technology and data security purposes (such as system backup, network performance monitoring, software license monitoring and computer asset tracking). UNSW College undertakes this support on a continuing and ongoing basis.
- (d) UNSW College reserves the right to inspect material on its ICT Resources when investigating an alleged breach or when required to comply with a formal request for legal disclosure (e.g. subpoena).

- (e) There are a number of circumstances in which UNSW College requires access to (as opposed to monitoring of) Student's electronic information, including email. These circumstances may include:
- (i) for network administration purposes;
  - (ii) to comply with court orders, for use in legal proceedings and/or to cooperate with investigations by law enforcement agencies; and
  - (iii) to ensure that use of the ICT Resources complies with the law and this Policy.
- Any disclosure of the results of such access will be in accordance with applicable legislation.

## 5.8. Breach of Policy

- (a) Breach of this Policy may constitute Non-Academic Misconduct and may result in disciplinary action taken in accordance with the [UNSW College Student Misconduct Policy](#).
- (b) Depending on the nature and severity of the breach, penalties or outcomes may range from loss or restriction of access to ICT Resources, to formal disciplinary action such as expulsion from the Program.
- (c) Any misuse of ICT Resources by Students may also attract financial penalties in addition to other disciplinary action. Cases of serious, deliberate, and/or criminal breach will be referred to external authorities and may result in civil or criminal proceedings.
- (d) If any Student becomes aware of or suspects a breach of this Policy, they should contact their teacher or Student Services. Any such contact will be treated as confidential, and any information disclosed will be properly investigated.

## 6. Legal and Policy Framework

### 6.1. Responsibilities

- (a) *Approver*  
The Chief Executive Officer is responsible for the approval of this policy.
- (b) *Responsible Officer*  
The Head of Information Technology is responsible for the implementation, dissemination and review of this policy.
- (c) *Contact Officer*  
The IT Helpdesk Team Leader is responsible for the day to day implementation of this policy and is the first point of contact for all enquiries that relate to this policy.
- (d) *Policy and Compliance Officer*  
The Policy and Compliance Officer is responsible for the administration and publishing of this policy.
- (e) *Staff, Supervisors and Executives*  
UNSW College staff, supervisors and executives are responsible for assisting in the implementation of and adherence to this policy.

## 6.2. Review

This Policy is due for review three (3) years from its date of implementation or in case of legislative or regulatory changes.

## 7. Related Documentation

N/A

## 8. Related Policies and Procedures

- (a) [UNSW Acceptable Use of UNSW Information and Communication Technology \(ICT\) Resources Policy](#)
- (b) [UNSW Student Code of Conduct](#)
- (c) [UNSW College Student Misconduct Policy](#)

## 9. Version History

| Version Control | Date Effective | Approved By | Amendment Notes |
|-----------------|----------------|-------------|-----------------|
| 1.0             | See page 1     | See page 1  | N/A             |