



Student Acceptable Use of ICT Facilities Policy

Policy number	TEC 1.01
Policy name	Student Acceptable Use of ICT Facilities Policy (Issue Two)
Applicability	All Bond University students
Contact person	PVC, Information
Policy status	Approved policy
Date of approval	4 October 2004
Date last amended	31 March 2008
Date of next review	31 March 2010
Related policies	TEC 1.08 Student ICT Account Policy TLR 6.01 Copyright Policy Part 3 University Handbook Discipline Regulations Part 3 University Handbook Student Conduct Code (page 13)

1. Overview

Student users of all or any of the computing and network systems, facilities and services are bound by certain rules which are outlined in this policy. Failure to comply with these rules may lead to the application of penalties, also outlined in this policy.

2. Definitions

Computing and network systems	Includes LANS, wireless and modems on the campus telephone system
Facilities	All computing facilities and services, provided in laboratories, lecture theatres, residences and other areas on campus and services provided through remote access from off campus.
Spoofing	The act of constructing electronic communications to appear as though they came from another party
Snooping	The act of monitoring the usage of any computer facility or the traffic generated by another user
Spam	<p>Unsolicited electronic communications. Examples of spam include, but are not limited to:</p> <ul style="list-style-type: none"> • Unauthorised mass email messages of a commercial, political, lobbying, unauthorised or fundraising nature • Forwarding chain letters or electronic “petitions”, or asking recipients to forward messages • Soliciting support (financial or otherwise) for charity, or special causes not connected with Bond University • Sending unverified public service announcements (such as virus alerts, unsafe products, lost and found, etc.), <p>Where e-mail messages, otherwise viewed as spam, are sent to as is appropriate to a university electronic mailing list, they may not necessarily be classed as spam.</p>
Hacking	The act of gaining unauthorised access to university computers, networks, information systems and / or other user accounts, via a local or remote communication network.

3. The Policy

Any variation to this policy for the education purpose of the University must be approved by the PVC, Information.

3.1 Agreement to this policy

- 3.1.1 All students are required to agree to the terms and conditions of the Student Acceptable Use Agreement when logging on to any University computer, signifying that they have read and agree to abide by the conditions outlined in this agreement.

3.2 Use of Facilities

- 3.2.1 Computer accounts are allocated to a student for their exclusive use while enrolled at Bond University. Accounts will be terminated if a student is not enrolled, or is not participating in a registered (with Academic Services) study program at another university.
- 3.2.2 Hardware and software are provided by Bond University for the purpose of academic pursuit. The use of facilities for consulting, personal gain, or any other purpose not directly related to academic pursuit is expressly forbidden. Limited non-commercial personal use is permitted.
- 3.2.3 Students are not to abuse, through excessive use, any facilities made available to them. The University reserves the right to impose limitations on the use of information resources, such as Internet downloads.
- 3.2.4 Students are required to manage their allocated network disk quota including email accounts, keeping within the quota limits allocated. See [Student ICT Account Policy](#).
- 3.2.5 Students must not use the facilities for any unlawful purposes including any purpose that relates to obscene, vulgar or harassing behaviour.
- 3.2.6 Students must not reserve or lock computer workstations, thereby preventing other users from using the unattended workstation.
- 3.2.7 Students must not bring food or drink into laboratories, or consume food or drink around or near any University workstations.
- 3.2.8 Students are required to abide by all laboratories and lecture theatre access rules and procedures. Where special access is provided, students are to take all responsibility for loss or damage of facilities under their charge.

3.3 Electronic Communication

- 3.3.1 Official correspondence from the University will be forwarded to students' Bond email account, and must be monitored by the student. Email accounts must be managed to remain within the quota storage requirements. See [Student ICT Account Policy](#).
- 3.3.2 Electronic communications must not be constructed to appear as though they came from another party, or from an anonymous source.
- 3.3.3 University email services must be used for University purposes only. Limited non-commercial personal use is permitted.
- 3.3.4 University email services must not be used to send spam. Information Services reserves the right to determine at its sole discretion (1) by reference to the definition of "spam" found above (see 2), what constitutes spam and (2) what measures are necessary in response to spamming complaints.

3.4 Email

3.4.1 Email is not private. Students acknowledge that it:

- Belongs to Bond University;
- May in certain circumstances be accessed by Bond University;
- Uses Bond University's name and address and therefore implies the sender is speaking with the authority of Bond University; and
- May in certain circumstances be inspected by parties outside of Bond University, for example, in the event of litigation.

3.4.2 Students agree not to construct electronic communications to appear as though they came from another party ("spoofing").

3.4.3 Students acknowledge that official correspondence from the University will be forwarded to their Bond email account, and that they agree to monitor their account. This includes, but is not limited to, notice or consent from a Manager, Dean or Vice-Chancellor. Notice will be taken to have been given once an email is sent unless an email is received shortly thereafter indicating that email delivery failed.

3.4.4 Students agree to use the University email system responsibly and appropriately and in accordance with all guidelines set out in this policy and the Student Conduct Code. Other than appropriate use of University mailing lists, students agree not to:

- Transmit threatening, defamatory, obscene or offensive materials;
- Send mass or unsolicited email messages of a commercial, political, lobbying or fundraising nature unless authorised and in furtherance of University business. Without limiting the generality of the foregoing, students agree that they will not use the facilities to perform acts which breach the [Spam Act 2003 \(Cth\)](#);
- Forward chain letters or electronic "petitions", or ask recipients to forward such messages;
- Solicit support (financial or otherwise) for charity, or special causes not connected with Bond University;
- Send unverified public service announcements (such as virus alerts, unsafe products, lost and found, etc.);
- Put anything in an email that cannot be repeated to anybody else or put in a hard copy memo.

3.5 Copyright, Illegal and Objectionable Material

3.5.1 Students must not copy or participate in any activity which involves copying Bond University software onto removable/portable media without authorisation from the copyright owner. Any such action is in breach of the law and against the policy of Bond University, and such actions can expose the student/s to appropriate disciplinary measures (see 3.8 below).

3.5.2 Students are forbidden from unlawfully copying onto Bond University storage systems, or unlawfully accessing or downloading using Bond University facilities, or using any Bond University facilities in any way to assist with the acquisition, distribution, broadcasting or public screening of any software or other copyright protected material (eg, MP3, DVD) licensed to other persons and/or organisations. This includes using shared drives of computers on the campus or residence networks to provide access to, or to distribute such material, whether the drive is freely accessible or password protected, regardless of who the owner of the computer is.

- 3.5.3 Students must not copy onto Bond University storage systems, or access using Bond University facilities, or use any Bond facilities in any way to assist with the acquisition or distribution of, any illegal material, or any material considered obscene or objectionable in nature or content. This includes using shared drives of computers on the campus or residence networks to provide access to, or to distribute such material, whether the drive is freely accessible or password protected, regardless of who the owner of the computer is.
- 3.5.4 Under Australian copyright law, unauthorised duplication and distribution of software can expose Bond University to fines and claims for civil damages, and expose the student to fines, together with possible jail terms and claims for civil damages. See also [Copyright Policy](#).

3.6 Security

- 3.6.1 Students are not to attempt to access areas of any facilities for which authority has not been granted.
- 3.6.2 Students must maintain facility security at all times and to immediately report any security breaches to Campus Security on 5595 1234. This refers to all aspects of facility security including, but not limited to, the physical security of computing equipment to which students have access and the integrity of any of the campus computer systems.
- 3.6.3 Students must not divulge passwords to any other persons and are to take reasonable precautions against the discovery of passwords by other persons.
- 3.6.4 Students are to take full responsibility for activities conducted using their computer and network accounts, and agree not to allow anyone else to use any of these accounts, and agree not to use any other person's accounts.
- 3.6.5 Students must not permit or aid unauthorised persons to use Bond University computing facilities. These facilities are for use by staff and enrolled students only.
- 3.6.6 Students are to protect the security of accounts to which they have access, ensuring that the system is logged out before leaving the computer which has been used to connect to the University service, whether that computer be locally or remotely connected to the University service.
- 3.6.7 Students must not monitor the usage of any computer facility or the traffic generated by another user.
- 3.6.8 Bond University system administrators may access a student's accounts, email and storage areas where necessary for facilities maintenance, to ensure the security and integrity of the computing facilities, and to provide access to Bond staff to data considered to be the property of the University.
- 3.6.9 Student computing activities will be logged and these logs will be used by systems administrators to ensure the security and integrity of the computing facilities.
- 3.6.10 Students must not attempt to use any tools, technologies or systems to conceal any behaviour on their part, or the part of another, that contravenes this policy. Information Services has the right to counter those tools, technologies or systems, in order to assess breaches of this policy and to protect University systems.

3.7 Tampering

- 3.7.1 Students must not interfere or attempt to interfere with the operation of any computing facilities, including hardware, software, files, and access by authorised users.
- 3.7.2 Students must not download, install, delete or modify software on Bond University facilities without authorisation from Information Services.
- 3.7.3 Students must not connect, disconnect or modify hardware on Bond University facilities without Information Services' authorisation. Privately owned computing equipment must not be connected to the Bond network without Information Services' authorisation.

- 3.7.4 Students must not operate any server or device that may compromise the operation of the Bond University network (including but not limited to DHCP, DNS, WINS, email, domain controller or LDAP server), on their computer, from any port on the network including those in the Bond University student residences, without the express approval of the Director, Information Services. Where such servers are found to be running and interfering with the operation of the University network, penalty procedures will be applied.

3.8 Indemnification

- 3.8.1 Students will indemnify the University for any loss caused by their breach of these rules including but not limited to a breach of any third party's intellectual property rights.

3.9 Breach of the rules and penalties

- 3.9.1 Breaches of the policy may be treated as misconduct under the [Bond University Disciplinary Regulations](#).
- 3.9.2 Breaches will be categorised according to their impact, their severity, and the incidence of repeat offences. Penalties for breaches could involve:
- Warnings;
 - locking of the user's account until they make contact with Information Services and are counselled;
 - extended suspension of account and lab access;
 - fines;
 - suspension or expulsion from the University;
 - referral to the authorities in relation to criminal proceedings.
- 3.9.3 Academic staff, security officers, Information Services staff and other administration staff are authorised to reinforce and police the student acceptable use policy.
- 3.9.4 Where a breach has been committed from a student's computer connected to the Bond University network, Information Services may disable the network port to which the computer is connected.

4. Related procedures

Nil

5. Related forms and guidelines

[Student Acceptable Use agreement](#)
[Student Acceptable Use penalty procedures](#)

Student Acceptable Use Penalty Guidelines

Penalties will apply in accordance with Bond University Disciplinary Regulations Section 12 (1) d, (3) g and 3 (o).

Following is a table of examples of offences and possible penalties.

Penalties are to vary with the seriousness of the offence, for example:

- Harassment – penalty may vary from apology for sending rude email, to referral to authorities for legal proceedings for threats, sexual harassment or stalking using electronic media.
- Hacking – penalty may vary from suspension of account for tampering with an account, to criminal charges for hacking into administrative computers to change or delete records.