STUDENT ACCEPTABLE USE OF ICT FACILITIES POLICY

Policy number	TEC 1.01
Policy name	Student Acceptable Use of ICT Facilities Policy (Issue Three)
Applicability	All Bond University students
Policy owner	Director, Information Technology Services
Contact person	Director, Information Technology Services
Policy status	Approved Policy
Date of approval	4 October 2004
Date last reviewed	
Date last amended	20 August 2016
Date last exposed	20 June 2016
Date last reviewed	3 October 2017
Date of next review	20 August 2019
Related policies	Copyright Compliance Policy (TLR 6.01) Social Media Policy (COR 4.03) Part 3 University Handbook Discipline Regulations Student Code of Conduct

1. OVERVIEW

Bond University provides ICT services to Bond University Students (Students) in order to assist students in their studies. In order to access these services, all students are allocated a Student Network Account once they are admitted to a program (see Student ICT Account Procedures).

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, Procedures and Guidelines.

2. THE POLICY

2.1. Variation

Any variation to this Policy must be approved by the Director, Information Technology Services. Variations will generally be approved only for the purposes of improving educational or student experience outcomes.

2.2. Agreement to this Policy

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

2.3. Use of Facilities

2.3.1. A student network account is allocated to a student for their exclusive use while enrolled at Bond University. Student network accounts may continue to be used for limited purposes after student enrolment has ended.

2.3.2. 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 where usage does not impact University infrastructure and/or services is permitted. Any personal use is subject to all Bond University policies governing ICT, including data collection, monitoring, analysis and liabilities.

2.3.3. 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 and data storage (see Use of Wireless Technology on Campus Guidelines).

2.3.4. Students are required to manage their allocated network disk quota including email accounts, keeping within the quota limits allocated. See Student ICT Account Procedures.

2.3.5. Students must not use the facilities for any unlawful purposes including any purpose that relates to obscene, vulgar, or harassing behaviour.

2.3.6. Students must not reserve or lock computer workstations, thereby preventing other users from using the unattended workstation.

2.3.7. Students must not bring food or drink into laboratories, or consume food or drink around or near any University workstations.

2.3.8. Students are required to abide by all laboratory 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.

2.3.9. Bond University reserves the right to monitor or review information stored on the facilities as well as Internet and email as necessary. Material communicated and received through the facilities is the property of Bond University and may be checked by others and/or deleted. Bond University reserves the right to prevent communications to and from external persons in its sole discretion. Users should hold no expectation of privacy while using University owned or leased equipment.

2.4. University Correspondence

2.4.1. Official correspondence from the University will be forwarded to the student's Bond email account, which must be monitored by the student. This includes, but is not limited to, notice or consent from a Manager, Executive Dean, Vice President, Deputy Vice-Chancellor, or Vice-Chancellor. Notice will be taken to have been given once an email has been delivered to a student account. Students acknowledge that they accept responsibility for managing their student email account so that official correspondence is read soon after it is received. Students acknowledge that they accept responsibility to ensure official correspondence is read and enacted upon prior to deadlines existing for the purposes of enforcing penalties.

2.4.2. Electronic communications must not be constructed to appear as though they came from another party, or from an anonymous source.

2.5. Email

2.5.1. 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.

2.5.2. University email services must be used for University purposes only. Limited non-commercial personal use is permitted provided that:

- all guidelines set out in this Policy are complied with; and
- use of Bond University's system for personal email is reasonable and not excessive.

2.5.3. Email accounts must be managed to remain within the quota storage requirements. See Student ICT Account Procedures.

2.5.4. Students must not construct electronic communications to appear as though they came from another party (spoofing).

2.5.5. University email services must not be used to send spam. Information Technology Services reserves the right to determine, at its sole discretion: (1) what constitutes spam; and (2) what measures are necessary in response to spamming complaints.

2.5.6. 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 Code of Conduct (Schedule B, *Student Handbook Part 3: Discipline Regulations*). 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.

2.6. Electronic Communication including Social Media and Social Networking

Bond University recognises the value of social media and social networking in education; however, use of the technologies can potentially create legal and ethical dilemmas, especially when on-line behaviour is unprofessional (or unlawful). (Refer to Social Media Policy)

2.6.1. Students, whilst using Bond University network, shall not participate in social networking activities which use language (text, audio, or video) or images which portray, or can be interpreted to portray, the following:

Illegal activities, intoxication, harassment, profanity, obscenity, pornography, abuse of people or animals, defamatory or libellous matter, threats, infringement of intellectual property rights, invasion of privacy, hate, discrimination, embarrassment to any person or entity, or matter otherwise injurious, objectionable, or inhospitable to professionalism or the image of Bond University.

2.6.2. Students, whilst using Bond University network, shall not post content that is libellous or defamatory as this puts the author at risk of civil legal action (amongst other potential penalties, including job termination, failure to secure employment, University disciplinary action).

2.7. Copyright, Illegal and Objectionable Material

2.7.1. 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 2.10 below).

2.7.2. 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 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 the owner of the computer.

2.7.3. 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 the owner of the computer.

2.7.4. Under Australian copyright law, unauthorised duplication and distribution of copyright protected material, including books, films, television shows, music or 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 Compliance Policy.

2.8. Security

2.8.1. Students are not to attempt to access areas of any facilities for which authority has not been granted.

2.8.2. 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.

2.8.3. Students must not divulge passwords to any other persons and are to take reasonable precautions against the discovery of passwords by other persons. See Password Management Procedures

2.8.4. 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.

2.8.5. 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.

2.8.6. 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.

2.8.7. Students must not monitor the usage of any computer facility or the traffic generated by another user.

2.8.8. Bond University system administrators may access a student's ICT account, email, and storage areas where necessary for facilities maintenance, to ensure the security and integrity of the computing facilities, and to provide Bond University staff access to data considered to be the property of the University.

2.8.9. 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.

2.8.10. 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 Technology Services has the right to counter those tools, technologies, or systems, in order to assess breaches of this Policy and to protect University systems.

2.9. Tampering

2.9.1. Students must not interfere or attempt to interfere with the operation of any computing facilities, including hardware, software, files, and access by authorised users.

2.9.2. Students must not download, install, delete, or modify software on Bond University facilities without authorisation from Information Technology Services.

2.9.3. Students must not connect, disconnect, or modify hardware on Bond University facilities without Information Technology Services' authorisation. Privately owned computing equipment must not be connected to the Bond network without Information Technology Services' authorisation.

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

2.10. Indemnification

2.10.1. 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.

2.11. Breach of the rules and penalties

2.11.1. Breaches of the Policy may be treated as misconduct under the Bond University Discipline Regulations

2.11.2. Breaches will be categorised according to their impact and severity, and the incidence of repeat offences. Penalties for breaches could involve:

- Warnings;
- locking of the user's account until they contact Information Technology Services and are counselled;
- extended suspension of account and laboratory access;
- fines;
- suspension or expulsion from the University;
- referral to the authorities in relation to criminal proceedings.

Penalties will 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.

2.11.3. Academic staff, security officers, Information Technology Services staff and other administration staff are authorised to reinforce and police the Student Acceptable Use Policy.
Where a breach has been committed from a student's computer connected to the Bond University network, Information Technology Services may disable the network port to which the computer is connected.

3. DEFINITIONS

Computing and network systems	Includes all Information and Communication Technology (ICT) hardware and software, and the systems they form.
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.
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. Includes the act of using ICT facilities and services with malicious intent in the absence of a breach of access restrictions.
Snooping	The act of monitoring the usage of any computer facility or the traffic generated by another user
Social Media	Media for social interaction, using highly accessible and scalable communication techniques. Social media uses web-based and mobile technologies to convert communication into interactive dialogue. Examples include Facebook, blogs, podcasts, discussion forums, RSS feeds, YouTube, interactive geolocation, online collaborative information, and publishing systems that are accessible to internal and external audiences, as well as related future technologies.
Social Networking	The use of dedicated websites and applications to communicate with other users, or to find people with similar interests to one's own. (Oxford Dictionary)
Spam	Unsolicited electronic communications. Examples of spam include, but are not limited to: ▪ 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.),

Where e-mail messages are sent to students, as is appropriate to a University electronic mailing list, they may not necessarily be classed as spam.

Spoofing The act of constructing electronic communications to appear as though they came from another party

4. RELATED PROCEDURES, FORMS AND GUIDELINES

Student ICT Account Procedures
Password Management Procedures
Use of Wireless Technology on Campus Guidelines
Bond University Student Logon Agreement – This reflects the content of this Policy and is agreed to by online click-through when logging in to the University network.

STUDENT ICT ACCOUNT PROCEDURES

1. CREATION OF STUDENT ACCOUNTS

Student Network Accounts are automatically created when the student is admitted to an approved study program of the University. These accounts enable access to various technology facilities provided by the University.

It is the responsibility of the student to activate their Student Network Account through an activation portal supported by Information Technology Services. The details of the activation portal are included in the enrolment information sent to students prior to the commencement of the semester. Information and assistance are also available from Information Technology Services.

2. STORAGE QUOTAS

2.1. Personal Home Drive Storage

Students are allocated a personal home (H) drive with a storage capacity of 250MB.

Students will receive automated alerts when usage of the H Drive approaches and exceeds 95% of the storage limits. If usage of the H Drive reaches 100% of the storage limits, the affected student(s) will no longer be able to save data to the H Drive.

2.2. Email Storage

Students are allocated an email account that also has a storage capacity of 50 Gigabytes.

Students will receive automated alerts when usage of the email storage approaches and exceeds 49 Gigabytes. As the usage of the email storage reaches 49.5 Gigabytes, students will not be able to send email, but will continue to receive email. As the usage reaches 50 Gigabytes, students will not be able to receive or send email.

Students should contact Information Services for advice and assistance with archiving their H drive data or email data.

2.3. OneDrive Storage

Students are allocated OneDrive storage with an initial capacity of 1024 gigabytes. Students are required to request additional storage if the initial capacity is filled.

2.4. Password Resets

Students can register for Self Service Password Reset at https://reset-registration.bond.edu.au and once complete, can reset their password at https://reset.bond.edu.au. Students may also contact Information Technology Services if they require their Student Network Account password to be reset.

2.5. Account disablement and deletion

Continuing Student accounts may be disabled for any of the following reasons:

- Non-payment of fees or charges, on advice from Financial Services or the Deputy Vice-Chancellor (Student & Support Services).
- Breach of the Student Acceptable Use of ICT Facilities Agreement.
- Breach of the Information Security Policy

3. DEFINITIONS

Account disabled	Account temporarily unavailable for use by the student.

USE OF WIRELESS TECHNOLOGY ON CAMPUS GUIDELINE

1. Overview

The purpose of this Guideline is to secure and protect the information assets owned by Bond University. Bond University provides computer devices, networks, and other electronic information systems to meet its business requirements. Bond University grants access to these resources as a privilege and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets.

This Guideline specifies the conditions that wireless infrastructure devices must satisfy to connect to the on campus wireless network. Only those wireless infrastructure devices that meet the standards specified in this Guideline or are granted an exception by Information Technology Services are approved for connectivity to the on campus wireless network.

2. General Network Access Requirements

Any use of communications technology on the campus, such as Bluetooth, cordless phones, and 802.11 wireless systems, using the 2.4GHz or 5GHz frequency bands must:

a) be authorised by Information Technology Services;
b) use Bond University approved authentication protocols and infrastructure;
c) use Bond University approved encryption protocols;
d) maintain a hardware address (MAC address) that can be registered and tracked;
e) not interfere with wireless access deployments maintained by other support organisations.

3. Laboratory and Isolated Wireless Device Requirements

All laboratory wireless infrastructure devices that connect to the on campus wireless network must adhere to section 2.1. Laboratory and isolated wireless devices that do not connect to the on campus wireless network must:

a) be isolated from the Bond University Corporate Network and on campus wireless network;
b) not interfere with the on campus wireless network.

4. Additional Guidelines

a) Bond reserves the right to use the following 802.11 protocols on campus to deliver wireless services to staff and students:
   - 802.11b/g/n/ac wireless technology operating at 2.4GHz;
   - 802.11a/n/ac wireless technology operating at 5 GHz.
b) The use of all cordless phones must be authorised by Information Technology Services. Some cordless phones operate in the 2.4GHz and 5 GHz bands and permission to use these will not be granted. Some cordless phones operating at 900MHz may be suitable for use.
c) If interfering technology is found to be in use, the owners will be required to cease its use. Although use on campus may not cause an immediate problem, it may do so as the wireless network is expanded.
d) Unauthorised installation of 802.11 systems is not permitted.
e) Use of wireless technology for research projects will be subject to the Executive Dean's approval if the use is outside the scope of this Guideline.

5. Definitions

Wireless technology Communications equipment which works using radio frequencies, and does not rely on cable connections.

PASSWORD MANAGEMENT PROCEDURE

1. Overview

The purpose of this Procedure is to establish a standard for the creation of secure passwords, the protection of passwords, and the frequency of password change.

Passwords are an important aspect of information security. They are the front line of protection for most computer systems. A poorly chosen password may result in the compromise of the Bond University corporate network. As such, all Bond University staff (including all third parties such as contractors and vendors with access to Bond University systems) are responsible for taking the appropriate steps, as outlined below, to ensure their passwords are secure.

Bond University uses a role-based approach for password management. Based on their role in the University, each staff member will be assigned to a security profile, and each security profile has an associated password guideline. If an individual has several roles, with conflicting password guidelines, the "strongest" guideline applies.

2. General

a) Three levels of password guidelines are used, each with a different set of requirements for password creation and reset, and these are described in the password guideline matrix.
b) The assignment of a password guideline is based on an individual's role(s) at the University and is not an automatic result of an affiliation or staff position.
c) All passwords must be changed as per the password guideline matrix. This will be enforced at the operating system level i.e. Windows, and at the application level, where possible (this will be dependent on system capabilities).
d) Passwords must not be inserted into email messages or other forms of electronic communication.
e) Password guidelines and security roles, and the resulting association of password guidelines to a user, are managed by Information Technology Services.

3. Password Protection Standards

All passwords are to be treated as sensitive, confidential Bond University information. The following password standards should be adhered to:

a) Do not reveal a password over the phone to ANYONE;
b) Do not hint at the format of a password (e.g., "my family name");
c) Do not reveal a password on questionnaires or security forms;
d) Do not share a password with family members;
e) Do not reveal a password to co-workers while on vacation;
f) Do not use the "Remember Password" feature of applications (e.g., Outlook, Internet Explorer);
g) Do not store passwords in a file on ANY computer system (including mobile devices) without encryption;
h) Temporary passwords should be changed at first log on;
i) If a password has been compromised or there is a possibility it may have been compromised then users should change their password immediately.

4. Application Development Standards

Application developers must ensure their programs adhere to the following security guidelines:

- Applications should support authentication of individual users, not groups;
- Applications should not store passwords in clear text or in any easily reversible form;
- Applications should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

5. Exclusions

- Infrequently there are certain circumstances whereby a particular vendor, technology or business process is unable to comply with this policy.
- Information Technology Services reserves the right to approve exceptions through a case-by-case review process, requiring final sign-off from either the Information Security Manager or Director, ITS.

6. Related Guidelines and Forms

Password Construction Guidelines and Matrix

PASSWORD CONSTRUCTION GUIDELINES

All Bond University Staff should ensure they select **strong** passwords. Strong passwords have the following characteristics:

a) Contain both upper and lower-case characters (e.g., a-z, A-Z);

b) Have digits and/or punctuation characters as well as letters (e.g., 0-9, @#$%^&*()_+|~-=\`{}[]:";'<>?,./);

c) Are at least eight alphanumeric characters long and is a passphrase (Ohmy1stubbedmyt0e);

d) Are not words in any language, slang, dialect, jargon, etc.;

e) Are not based on personal information, names of family, etc.;

f) Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is to create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

Poor or weak passwords have the following characteristics:

a) The password contains less than eight characters;

b) The password is a word found in a dictionary (English or foreign);

c) The password is a common usage word such as:

   i. Names of family, pets, friends, co-workers, fantasy characters, etc.;

   ii. Computer terms and names, commands, sites, companies, hardware, software;

   iii. The words "Bond University", "Robina", "Gold Coast" or any derivation;

   iv. Birthdays and other personal information such as addresses and phone numbers;

   v. Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.;

   vi. Any of the above spelled backwards;

   vii. Any of the above preceded or followed by a digit (e.g., secret1, 1secret).

Password Guideline Matrix

Name	Description	Example
Level 0	Standard	Students, Vendors/Guests
Level 1	Medium	Staff
Level 2	High	Chancellery, DVCs, Executive Directors, Executive Deans, Faculty Business Directors (Typically all staff on executive contracts)

Attribute	Level 0	Level 1	Level 2
Minimum length of password	8	8	8
Maximum age of password (in days)	365	365	90
Days of daily expiration warnings	14	14	14
Password minimum age for reset (in days)	0	0	0
Password uniqueness/history	5	5	5
Failed attempts before lockout	5	5	5
Password Complexity	False	True	True