BOND UNIVERSITY	**INFORMATION COMMUNICATION TECHNOLOGY ACCEPTABLE USE POLICY**
Contact Officer	Director, Information Technology Services
Date First Approved	4 October 2004 (as Student Acceptable Use of ICT Facilities policy) 16 November 2006 (as Staff Acceptable Use of ICT Facilities policy)
Approval Authority	Director, Information Technology Services
Date of Next Review	24 January 2026

1. PURPOSE AND OBJECTIVES

Bond University provides its Authorised Users with secure and timely access to Information Communication Technology (ICT) services to facilitate learning and teaching, research, engagement, administration and other functions of the University.

This Policy is intended to:

- provide a clear statement of responsibilities for all Authorised Users of University ICT Services, including what constitutes acceptable and unacceptable use;
- ensure that Authorised Users do not adversely impact the University's operations, assets or reputation;
- outline the provision, modification, and removal of access to University ICT Services; and
- express the commitment of the University to maintaining secure, effective, and reliable University ICT Services.

2. AUDIENCE AND APPLICATION

- This Policy applies to all Authorised Users of the University ICT Services managed by the University or third-party providers on behalf of the University, both on and off campus.
- University ICT Services are the property of the University. Anything sent or received using the network, systems, services and facilities of the University will therefore be transmitted and stored on university property (or on third party property on behalf of the University).

3. ROLES AND RESPONSIBILITIES

Role	Responsibility
Director, ITS	Approve any variation to this policy. Generally, variations may only be approved for the purposes of improving educational or student experience outcomes whilst maintaining secure, effective and reliable ICT Services
University Librarian	Ensure and enforce copyright compliance with the Copyright Act 1968 (Cth)

4. POLICY STATEMENT

4.1. Agreement to this Policy

4.1.1. Authorised Users are required to agree to the terms and conditions of this Policy when signing into any University computer or service, signifying that they have read and agree to abide by the conditions outlined in this Policy.

4.1.2. Authorised Users must act in accordance with this Policy and all other applicable University policies and procedures,

4.2. Acceptable Use of University ICT Services

4.2.1. University ICT Services and Authorised Users span multiple legal jurisdictions. Authorised Users have a responsibility to be aware of the jurisdiction that applies to their location when using University ICT Services.

4.2.2. Authorised Users are permitted to use University ICT Services for properly authorised and supervised business, education or research purposes, at a level that is commensurate with their position, role, delegated authority or student status, providing that the use:

i. Is lawful;
ii. Is in a responsible, ethical and equitable manner;
iii. Is consistent with the values of the University as outlined in the University's codes of conduct; and
iv. Does not adversely impact the University's operations, assets, or reputation.

4.2.3. Limited non-commercial personal use of University ICT Services is acceptable, providing that the use is otherwise in accordance with this Policy and where usage does not impact University operations, assets, or reputation. Any personal use is subject to all Bond University policies governing ICT, including data collection, monitoring, analysis, and liabilities.

4.2.4. University ICT Services must not be used in any manner which the University considers to be inappropriate. This may include, but is not limited to:

i. Knowingly downloading, storing, distributing or viewing of offensive, obscene, indecent, or menacing material. This could include, but is not limited to, pornography, defamatory or libellous material, material that could constitute racial or religious vilification, discriminatory material, material that incorporates hate, abuse of people or animals, invasion of privacy, intoxication, harassment, gratuitous violence or frequent and highlighted bad language;
ii. Unauthorised monitoring of electronic communications;
iii. Consulting, personal gain, or any other purpose not directly related to university pursuits;
iv. Stalking, blackmailing or engaging in otherwise threatening behaviour or communications;
v. Any use which breaches a law, including copyright breaches, fraudulent activity, computer crimes and other computer offences;
vi. Abuse through excessive use, data storage, downloads or CPU utilisation;
vii. Transmitting spam or other unsolicited communications including but not limited to chain letters or electronic 'petitions', or ask recipients to forward such messages;
viii. Solicit support (financial or otherwise) for charity or special causes not connected with the University;
ix. Using tools, technologies, or systems to conceal any behaviour on their part, or the part of another, that contravenes this Policy;
x. Gaining unauthorised access to University ICT Services (Hacking) via a local or remote communication network
xi. Send unverified public service announcements (such as virus alerts, unsafe products, lost and found);
xii. Using University data plans irresponsibly, when working from home users should utilise home Wi-Fi if available;
xiii. international roaming on mobile devices (prior Executive level approval required for any exceptions);
xiv. Constructing electronic communications to appear as though they came from another party, or from an anonymous source (Spoofing); or
xv. The introduction or distribution of security threats, including a virus or other harmful malware.

4.2.5. Storing personal data (including emails, documents, photos and videos) within Bond owned devices and services creates legal risk for Bond and employees. Employees are encouraged to separate personal data from work related data, by using personally owned devices for personal data. On termination of the recognised relationship with Bond, it is the Authorised User's responsibility to remove all personal data and email, including any personal intellectual property (as defined in the Intellectual Property Policy) from their accounts**.** Personal data and email used within Bond owned devices and/or services will remain within the Bond backup and recovery service.

4.2.6. Authorised Users who are unsure whether a proposed use is permitted or authorised should seek written approval from their supervising head of organisational unit (e.g., Executive Dean, Vice President, or Director)

4.2.7. Authorised Users must not attempt to gain unauthorised access to University ICT Services (and the information stored thereon) to which they have not been given access or permit others to do so (Note: kiosk services have an implicit authorisation to use).

4.2.8. Authorised Users must not tamper with University ICT Services that may potentially cause performance degradation, service instability, or compromise operational efficiency, security, divulging of information, or fair use.

4.2.9. Authorised Users must not reserve or lock any shared computer device, thereby preventing other users from using the unattended device.

4.2.10. In accordance with the IT Account Termination Policy, access to University ICT Services will be removed when the relationship between Authorised Users and the University ceases.

4.2.11. Authorised Users must not use their access to University ICT Services to gain inappropriate personal, academic, financial, or other advantage.

4.2.12. In accordance with the Information Security Policy, Authorised Users are not permitted to provide others with their Authentication Credential(s). It is the responsibility of Authorised Users to ensure that their Authentication Credentials are securely stored as they are responsible for all activity initiated or conducted from their account or with their Authentication Credential(s).

4.3. Monitoring and Privacy

4.3.1. Authorised Users must maintain, at all times, the confidentiality and privacy of any Personal Information accessed via University ICT Services.

4.3.2. The capture or storage (whether electronic or physical) of personal information must be limited to only that information that is required by that process to function or that which is required for legal or regulatory requirements and only for the duration required, with processes in place for secure deletion when no longer needed.

4.3.3. The capture or storage of credit card details or cardholder data, including on receipts or paper reports, is not permitted. All credit card processing must be through an authorised third-party service provider and/or payment gateway. All hardware payment processing is via a validated PCI-listed P2PE solution and the

only systems in our university environment that store, process, or transmit account data are the payment terminals from a validated PCI-listed P2PE solution.

4.3.4. The University reserves the right to monitor, access, log and analyse the activities of Authorised Users, and of all University ICT Services, and conduct reviews and audits as necessary.

4.3.5. The University reserves the right to prevent communications to and from persons in its sole discretion.

4.3.6. All Authorised Users must report any actual or suspected security weaknesses, breach or threat involving University ICT Services to the IT Service Desk or the Director, ITS as soon as possible.

4.3.7. Subject to the provisions of the University's Privacy Policy and relevant legislation, the University may disclose the contents of electronic communications without permission of the Authorised User.

4.3.8. The University reserves the right to block and/or filter any use that breaches this Policy or exceeds the University's acceptable level of risk**.**

4.3.9. Monitoring the usage of any University ICT Service or the traffic generated by an individual user (Snooping) is prohibited unless it is for the purpose of investigating or maintaining the security of the University ICT Services or prior authorisation has been granted by the Vice Chancellor or Vice President Operations.

4.3.10. The University may take any action deemed necessary to remedy immediate threats to University ICT Services or security including, without limitation, suspending an Authorised User's access, confiscation of University-owned devices and/or disconnecting or disabling equipment with or without prior notice.

4.4 Inadvertent Unacceptable Use

4.4.1 Authorised Users, who inadvertently receive, transmit or access material (for example, via email or the Internet) that may be considered Inappropriate Material and is not related to their work duties, must take immediate action to either delete such material or cease such access.

4.4.2 Advice must be sought from the Authorised User's supervisor or the IT Service Desk if Inappropriate Material continues to be received.

4.5 University Correspondence

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

4.6. Copyright, Illegal and Objectionable Material

4.6.1. Authorised Users (staff and students) must not use any Bond University ICT Services for an unlawful purpose, including, but not limited to the following;

- Copying or distributing Bond University software without authorisation.
- Copying or distributing any material which could be considered as obscene or objectionable in content or nature.

Such actions may result in the University applying appropriate disciplinary measures

4.6.2. Infringing copyright or any other intellectual property right in any way by copying, accessing or downloading, or assisting with the use, acquisition, distribution, broadcasting or public screening of, any copyright protected material including books, films, television shows, music, or software without the copyright holder's permission or licence.

4.6.3. Such action can expose Bond University to fines and claims for civil damages, and expose the staff member or student to fines, together with possible jail terms and claims for civil damages (see the University's Copyright Compliance Policy for further information).

4.7. Connected Devices

4.7.1. Authorised Users must not connect, disconnect, or modify hardware on University ICT Services without Information Technology Services' authorisation.

4.7.2. Privately owned devices must not be connected to the University wired computing network without Information Technology Services' authorisation and must support enterprise networking technology.

4.7.3. Authorised Users must take responsibility for the security of personally owned computers and equipment used in conjunction with the University's ICT Services.

4.7.4. Authorised Users must not operate any server or device on their computer, on the University network that may compromise the operation of the University network (including but not limited to DHCP, DNS, WINS, email, domain controller servers or network tunnelling such as reverse proxies, exit nodes or remote access), 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.

4.8. Consequences of breach

4.8.1. Breaches of this Policy may be grounds for misconduct or serious misconduct under the Bond University Discipline Regulations.

4.8.2. A breach or alleged breach of this Policy may result in a referral of the matter to the police and/or other relevant external authority.

4.8.3. Authorised Users 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.

4.8.4. Breaches will be categorised according to their impact and severity, and the incidence of repeat offences including copyright infringements. Penalties for breaches will vary according to the seriousness of the office and could involve:

- Immediate suspension of the Authorised User's account;
- Disabling network access to the connected device;
- Fines;
- Termination or expulsion from the University;
- Referral of the matter to the police and/or other relevant external authorities;

5. DEFINITIONS, TERMS, ACRONYMS

Authorised User	A person who has been provided with an Authentication Credential by the University to access University ICT Services.
Authentication Credential	User identification and password, username and passcode, PINs or other secret means to gain access to University ICT Services. Passwords used on all systems should comply with Bond's Password Management Procedures.
Electronic Communications	Any form of communication that is broadcast, transmitted, stored or viewed using electronic media, such as computers, phones, email, video, voice call, social media, electronic chat functions, social networks, etc
Facilities	All computing and telecommunication facilities provided in offices, meeting rooms, laboratories, lecture theatres and teaching spaces, residences and other areas on campus and services provided through local or 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 University ICT Services and services with malicious intent in the absence of a breach of access restrictions.
ICT	Information and Communication Technology
Inappropriate Material	Inappropriate Material means content that, if accessed through University ICT Services, contravenes the Information Communication Technology Acceptable Use Policy;
Personal Information	Any information or an opinion, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion. Refer to classification levels in the Information Security Policy for examples of sensitive data.
Snooping	The act of monitoring the usage of any University ICT Service 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.
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

University ICT Services — Facilities and/or Services provided to an authorised user (wired or wireless) including software, internet usage, email, communication devices, hardware and computing infrastructure under the control of the University (or a third-party provider on the University's behalf) that provides access to information in online or electronic format.

6. RELATED DOCUMENTS

Student ICT Account Procedures
Password Management Procedures
Use of Wireless Technology on Campus Guidelines
Bond University Logon Agreement – This reflects the content of this Policy and is agreed to by online click-through when signing into the University network
Copyright Compliance Policy
Social Media Policy
Student Code of Conduct
Intellectual Property Policy
Privacy Policy
Information Security Policy
Authorised Software Policy

7. MODIFICATION HISTORY

Date	Sections	Source	Details
24 January 2023		Director of ITS	▪ Combined separate Staff and Student policies into a single policy to further cater for all authorised users, not just staff and students ▪ New definitions added for "Authorised Users" and "University ICT Services"
19 November 2019			