# STAFF ACCEPTABLE USE OF ICT FACILITIES POLICY

| | |
|---|---|
| **Policy number** | TEC 1.04 |
| **Policy name** | Staff Acceptable Use of ICT Facilities Policy (Issue Four) |
| **Applicability** | All staff |
| **Policy Owner** | Director, Information Technology Services |
| **Contact person** | Director, Information Technology Services |
| **Policy status** | Approved Policy |
| **Date created** | 16 November 2006 |
| **Date last amended** | 19 November 2019 |
| **Date last exposed** | October 2019 |
| **Date last reviewed** | |
| **Date of next review** | 19 November 2022 |
| **Related policies** | Copyright Compliance Policy (TLR 6.01)<br>Intellectual Property Policy (TLR 6.02)<br>Staff Consultancy Policy (TLR 7.01)<br>Privacy Policy (COR 1.01)<br>Authorised Software Policy (TEC 2.02)<br>Social Media Policy (COR 4.03)<br>Enterprise Architecture Guiding Principles |

## 1. OVERVIEW

### Background

Information technology Facilities and resources are essential to the educational, research and administrative pursuits of Bond University. The University seeks to provide excellent Facilities for academic and professional staff, to protect both the Facilities and their users, and to ensure a productive and safe computing environment. It seeks to do this without imposing unnecessary restrictions that would detract from the University's culture of open enquiry.

### Purpose

The purpose of this Policy is to outline acceptable use of computing Facilities at Bond University, to enable staff to work confidently in the information technology infrastructure whilst safeguarding the integrity of the computer systems, networks, software, and data. Inappropriate use exposes Bond University to risks including attacks from malicious software, disruption and compromise of network systems and services, and legal issues.

### Scope

This Policy applies to the use of all Computing and Network Facilities and systems including wired, wireless, phone systems and Internet hosted services, computer rooms, data cupboards, equipment racks, Facilities and services provided in offices, laboratories, libraries, lecture theatres, residences and other areas on campus, and services provided through remote access from off campus, collectively referred to as the "Facilities".

### Breach

Staff agree to be bound by this Policy each time they access any of the Facilities for the duration of their use of the Facilities. The Facility "user" is taken to be the person logged on at the time. Any breach of this Policy may result in suspension or termination of accounts and/or disciplinary action up to and including dismissal.

## 2. THE POLICY

### 2.1. Agreement to this Policy

2.1.1. All Facility users, in an employment, contractor, consulting or visiting capacity, who are provided with any Bond University staff account (network, email, or application account), and/or with access to Bond University Facilities, are bound by this Policy and are deemed to be in a Recognised Relationship with Bond University and will be asked to sign a copy of the Staff Acceptable Use of ICT Facilities Policy to acknowledge their acceptance of the terms and conditions of this Policy before access is granted.

### 2.2. Use of Facilities

2.2.1. Staff must comply with all directions pertaining to the access and use of the Facilities issued by Bond University.

2.2.2. Staff Network Accounts are allocated to a staff member, for their exclusive use, whilst they have an employment, consulting, or visiting relationship (Recognised Relationship) with Bond University and will be terminated when the Recognised Relationship ceases.
2.2.3. Staff are to take full responsibility for activities conducted using their accounts and must not allow anyone else to use any of these accounts and agree not to use any other person's accounts.
2.2.4. All Facilities provided by Bond University to staff members remain the property of Bond University at all times. Staff must return all Facilities to Bond University immediately upon request to do so by Bond University and/or immediately upon the termination of the Recognised Relationship with Bond University.
2.2.5. Staff must not interfere or attempt to interfere with the operation of any computing Facilities (tampering), including hardware, software, files, and access by authorised users including using or propagation of computer malware. Staff are prohibited from engaging in social engineering of any nature which may lead any person to divulge information or take any action which would otherwise not occur under normal circumstances.
2.2.6. Only ICT staff or those with written authorisation are permitted to perform maintenance on the Facilities.
2.2.7. Staff may not operate any server or device that may compromise the operation of the Bond University network (including 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, ITS. Where such servers are found to be running, at the discretion of the Director, ITS, the network port for that device will be disabled, disconnecting that device from the network, and any associated user accounts will be disabled, pending removal of the offending device.
2.2.8. Bond University makes no express or implied warranties or conditions regarding the Facilities or Internet and assumes no responsibility for any consequence of service interruptions or changes or the receipt or delivery of any electronic communication.
2.2.9. On termination of the Recognised Relationship, it is the staff member's responsibility to remove all personal data and email, including any personal intellectual property (as defined in the Intellectual Property Policy) from their accounts. The staff member should make arrangements for all University data to be made available to other relevant employees. If there is data or email remaining in the staff member's account at the time of termination, the University may access and use such data for University purposes.
2.2.10. Bond University reserves the right to immediately, and without notice, withdraw or suspend access to the Facilities.
2.2.11. 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.
2.2.12. Facilities are provided by Bond University for the purpose of fulfilling staff employment responsibilities. Limited personal use is permitted for appropriate purposes. The use of Facilities for consulting must be in accordance with the Bond University Staff Consultancy Policy, and other use, such as for other business or personal gain not sanctioned by the University, is expressly forbidden.
2.2.13. Staff are to manage their allocated network storage and email quotas, keeping within the quota limits allocated to them. Requests for additional quota can be made to the Information Technology Services Service Desk.
2.2.14. Staff must not store data on local disk drives but use the allocated network disk space on shared drives which will be backed up to protect against hardware failure and data corruption.
2.2.15. Staff must abide by all laboratory, library and lecture theatre access rules and procedures. Staff must not bring food or drink into labs or consume food or drink around or near any workstations in a lab, or lecture room.
2.2.16. Bond University shall not be held responsible in any way for any content or information accessed via the Facilities.

### 2.3. Prohibited Activities

2.3.1. Software owned or licensed by Bond University is for use by the University. It is illegal to copy and distribute any such software by any means. Unauthorised duplication and distribution of software may expose Bond University to fines and claims for civil damages, and expose the individual to fines, together with possible jail terms and claims for civil damages.
2.3.2. Staff must not use any Facilities for an unlawful purpose, including, but not limited to, the following:

- Infringing copyright or any other intellectual property right in any way and by copying, accessing or downloading, or assisting with the use, acquisition, distribution, broadcasting or public screening of, any software or other copyright protected material without a licence (as outlined in the Copyright Compliance Policy).
- Using devices connected to the campus or residence networks to provide access to, or to distribute, infringing material, whether freely accessible or password protected, and whether the device is owned by Bond University, a staff member, a student, or another party (see Use of Wireless Technology on Campus Guidelines).

- Engaging in conduct that is defamatory or which amounts to discrimination or unlawful harassment. This includes, but is not limited to, the sending of unwanted email.
- Sending, receiving, storing, displaying, printing, uploading, downloading or otherwise disseminating material that is fraudulent, illegal, embarrassing, sexually explicit, obscene, intimidating, defamatory, racist, sexist, or generally inappropriate except when required for approved teaching or research purposes. While the University encourages critical analysis and review of cultural and social norms, it does not condone unlawful, insulting or demeaning behaviour. Staff members are expected to consider the sensitivities of other users.

2.3.4. Messages posted to discussion forums, social media and other online facilities must be in accordance with the written charters for those forums. The user is responsible for identifying and complying with the policies of a given forum before posting to it. Staff members must not disrupt or attempt to disrupt discussion forums by posting a large number of messages. Disruption occurs when normal discussion in the group is significantly hindered.

2.3.5. Staff members must not use the Facilities to perform any action that would bring Bond University into disrepute. This includes, but is not limited to, dispersing internal or confidential data without proper authorisation.

### 2.4. Security

2.4.1. Staff must not access or attempt to access any Facilities for which they do not have authority.

2.4.2. Staff must, at all times, take all reasonable steps to maintain Facility security and immediately report any security breaches to Information Technology Services or Campus Security.

2.4.3. Bond University computers must run Bond University's chosen anti-virus software. Staff must not attempt to disable or interfere with the anti-virus software and must report any instances in which they believe the software has been disrupted from normal operation to Information Technology Services.

2.4.4. Staff are responsible for activities conducted using their staff accounts. Any information or data stored by staff on University systems is the responsibility of the staff member who stored the information or data. Staff must take reasonable precautions against the discovery of their passwords by other persons and comply with any Bond University password polices that may be in force (see Password Management Procedures).

2.4.5. Staff should not permit or aid unauthorised persons to use Bond University computing Facilities.

### 2.5. Monitoring Facility Use

2.5.1. Bond University will conduct activity monitoring of all users and devices which access computing facilities and services for the purpose of:

- protecting its assets from suspected unlawful activities or activities which are in breach of University policy or rules;
- conducting its business and operational requirements;
- protecting its reputation; and
- compliance with legislative obligations.

2.5.2. Monitoring will be carried out by all means available to the University, including but not limited to:

- accessing University staff accounts or emails;
- accessing files;
- accessing work computers and/or other hardware, including activity logs;
- recording wired and wireless internet usage, including device type and location; and
- accessing telephone usage logs.

2.5.3. Bond University system administrators may access data gathered as a result of activity monitoring where necessary to ensure the security, integrity, and efficient operation of the Facilities.

2.5.4. At the discretion and upon written authorisation from the Vice Chancellor, Vice President Operations, or Executive Director, Strategy, Systems & People, Bond University system administrators may provide to other Bond staff a copy of data gathered as a result of activity monitoring (refer 2.5.2). ICT management will keep a record of all approved accesses.

2.5.5. Staff may 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. ICT management has the right to counter those tools, technologies, or systems, in order to assess breaches of this Policy and to protect University systems. This includes tools and technologies that enable the locking down of a computer to prevent remote access for systems administration and monitoring purposes.

2.5.6. Monitoring the usage of any computer Facility 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 Facilities or prior authorisation has been granted by the Vice Chancellor, Vice President Operations, Executive Director, Strategy, Systems & People.

### 2.6. University Correspondence

2.6.1. Official correspondence from the University will be forwarded to a dedicated Bond staff email account which must be monitored by the individual staff member. This includes, but is not limited to, notice or consent from the Manager, Executive Director, Executive Dean, Deputy Vice-Chancellor, Vice President, University Registrar, or Vice Chancellor. Notice will be taken to have been given once an email has been delivered to the staff email account.

2.6.2. In order to ensure appropriate use of the University's most comprehensive distribution lists (i.e. those that include large numbers of staff or students) email distribution lists are moderated according to the criteria established in the Moderation of Email Distribution Lists Procedures.

### 2.7. Email

2.7.1. Staff must use the University email system responsibly and appropriately and in accordance with all guidelines set out in this Policy and the staff Code of Conduct Policy.

2.7.2. Email is not private. Staff members acknowledge that it:

- belongs to Bond University;
- may, in certain circumstances, be accessed by Bond University; and
- may, in certain circumstances, be inspected by parties outside of Bond University, for example, in the event of litigation.

2.7.3. Employees may send personal email, that is, non-work-related email, provided that:

- all guidelines set out in this Policy are complied with;
- use of Bond University's system for personal email is reasonable and not excessive; and
- use of email for personal matters most appropriately occurs outside of normal work hours, during lunchtimes, breaks or on weekends.

2.7.4. Staff must not construct electronic communications to appear as though they came from another party (Spoofing).

2.7.5. University email services must not be used to send Spam. ITS reserves the right to determine, at its sole discretion what constitutes Spam and what measures are necessary in response to spamming complaints.

2.7.6. On termination of the Recognised Relationship, all correspondence addressed to a staff member's email account, and all associated email addresses, may immediately be directed to other Bond University employees. Redirection of email to an ex-staff member's personal email account following termination will not be possible.

### 2.8. Telecommunications

Desk telephones are provided to enable staff members to perform their duties and to conduct the business of the University. The Telephone and Facsimile Procedures set out the conditions for use.

Mobile communication, including voice and data communication, is an integral part of daily university life. Bond University aims to use Mobile Communications Devices in a manner which assists employees to perform their responsibilities effectively and flexibly, ensures enhanced client service, while maintaining efficiency, safety, and fair and responsible use.

The Mobile Communications Devices Procedures establishes the set of conditions for the use of Mobile Communications Devices provided to designated employees by the University.

## 3. INDEMNIFICATION

Staff agree to indemnify the University for any loss arising out of a breach of the rules contained in this Policy and the associated Agreement, including but not limited to a breach of any third party's intellectual property rights.

## 4. DEFINITIONS

| | |
|---|---|
| **Computing and Network Facilities** | Includes all Information and Communication Technology (ICT) hardware and software, and the systems they form. |
| **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. |
| **ICT** | Information and Communications Technology |
| **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. |
| **Mobile Communications Device** | Includes mobile telephones, Blackberry devices, other smartphones, mobile broadband dongles, slates/tablets with embedded SIMs and other mobile data devices that utilise a cellular network for communication, whether voice or data communication. |
| **Recognised Relationship** | All staff, consultants, contractors, and other visitors engaged by Bond University who will be using the University's computing facilities are deemed to be in a recognised relationship with Bond University. |

**Snooping** The act of monitoring the usage of any computer Facility or the traffic generated by another user.

**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, otherwise viewed as spam, are sent to 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.

## 5. RELATED PROCEDURES, FORMS AND GUIDELINES

Staff Acceptable Use of ICT Facilities Agreement
Moderation of Email Distribution Lists Procedures
Telephone and Facsimile Procedures
Mobile Communications Devices Procedures
Password Management Procedures
Software Licence Monitoring Procedures
Use of Wireless Technology on Campus Guidelines
Use of Personal Cloud Data Storage Services Guidelines (ITS)

## MODERATION OF EMAIL DISTRIBUTION LISTS PROCEDURE

The University's most comprehensive Email Distribution Lists are moderated to ensure appropriate use.

Direct mailing to these distribution lists is limited to the Vice Chancellor and Vice President Operations only to send essential University announcements. The University Registrar, Director, Student & Academic Services and Director, Information Technology Services are also authorised to email the all_students distribution list regarding student enrolment and system-related matters.

Unmoderated lists can freely receive email from any internal Bond email address. A Faculty/Department can elect to moderate an email list and nominate appropriate moderators via a request to ITS.

**Email communication/moderation process**
A "Daily Digest" newsletter is sent to all staff and students each afternoon to consolidate and facilitate email communications. This newsletter is used to disseminate information, including:

- Administrative information from Faculty and Offices
- Scheduled maintenance notices from Facilities Management and Information Technology Services
- Internal job vacancies
- Changes to opening hours of services and offices
- Security notices
- Staff training announcements
- University-wide functions
- Bond community announcements

To submit a contribution to a Daily Digest, please complete the following online request via the Online Bond Support Portal. Submissions close each day at noon for an afternoon release.

## DEFINITIONS

| | |
|---|---|
| **Email Distribution List** | A list of e-mail addresses identified by an alias (or reflector) which is a single e-mail address. When a message is sent to the list alias, all members of the list receive a copy of that message. |
| **Moderation** | Moderation is employed to ensure that only those messages that meet the criteria for the list are delivered. A moderator must approve and forward every message sent to the list alias before successful delivery. |

## TELEPHONE AND FACSIMILE PROCEDURES

The use of Bond University's desk telephones for toll calls is permitted for business purposes where it is the most effective and efficient method of communication and alternative methods of communication (e.g. email or fax) are not appropriate.

Bond University incurs the cost of the telephone system and facsimile machines in order to conduct the University's official business. These are not provided for personal use and, because such personal use incurs an unplanned cost for the business, limited personal use is provided as a privilege. This occasional and brief personal use is permitted provided it is conducted in an expeditious manner and that the calls are local and no long-distance charges are incurred.

Where phones are toll barred, the staff member should obtain approval from the relevant manager to access another phone in the Faculty/Office that has the appropriate access. Alternatively, the manager may contact the Service Desk to request that access be increased for the particular phone.

Internal telephone extensions (landlines) should not be diverted to personal mobile phones, except in exceptional circumstances, as this escalates the cost to Bond University. On approval of the relevant Executive Dean/Director, an office extension may be diverted to a Bond mobile phone or smartphone device during a period of absence from the office. Voicemail is provided to all staff members to answer calls when away from the office. Voicemail can be delivered to an email inbox which enables messages to be accessed remotely. When travelling overseas, it is expected that calls will be diverted to voicemail or an appropriate colleague.

The cost of all fixed line communication is charged back to the individual cost centres within the University. The University reserves the right to recoup expenses incurred as a result of a staff member making excessive personal calls from University telephone extensions.

Private/personal interstate (STD) or international (IDD) calls may not be made from University extensions unless in an emergency situation and on approval by the relevant Executive Dean/Director.

In accepting a University desk telephone, staff members acknowledge the University's right to list their names in its telephone or other associated directories and to have the extension number and calling party displayed (with the exception that numbers that require confidentiality will have the extension number removed but will still have the calling party name displayed). Confidential numbers will only be issued if the case for confidentiality can be established prior to the number being allocated.

Staff must at all times comply with any legal requirements governing the use of telephones and facsimile equipment and should be aware that certain improper uses could constitute a criminal offence.

In addition to the requirements laid down by law, the University prohibits the use of company facsimile machines or telephones for:

- obscene or objectionable communications;
- harassment;
- conducting gambling or distribution of "chain letters";
- conducting any illegal activities;
- soliciting for personal gain or profit or conducting any personal commercial or commercially related activities.

# MOBILE COMMUNICATIONS DEVICES PROCEDURES

**Acquiring a mobile phone**
The allocation of a Mobile Communications Device for use by an academic or professional staff member is to be approved by the relevant Executive Dean/Director/Deputy Vice-Chancellor where there is an adequate need and there is sufficient benefit to the University.

A request for the purchase of a Mobile Communications Device should be forwarded to the Service Desk – Information Technology Services using the appropriate forms available from the Information Technology Services Intranet which are:

- Mobile Phone https://www.staff.bond.edu.au/its/forms/mobilecommunications.pdf
- Data Sim Only (for tablet and USB dongle)https://www.staff.bond.edu.au/its/forms/mobiledata.pdf

The Voice Communications Officer will then contact you with a price list for the brand you indicate on the form.

Both forms must be signed by the relevant Executive Dean/Director/Deputy Vice-Chancellor.

Circumstances in which the allocation of a Mobile Communications Device includes, but is not limited to, the following:

- There is a requirement for the staff member to undertake frequent out-of-office duties, including travel.
- There is a requirement for the staff member to be on call.
- There is a lack of access to a fixed telephone.
- The staff member has specific security or contact function.
- Improved productivity, enhanced client service or greater efficiency is possible through the flexibility offered by a Mobile Communications Device.

**Fair and Responsible use**
The use of telephones must be as cost effective as possible. The following principles must be observed:

- The number of calls made should be limited to those necessary for effective business.
- Calls are to be brief.
- Mobile telephones should not be used when teaching class, at meetings or in the Library.
- Mobile telephone batteries are to be properly maintained to ensure long service life.
- Reasonable care must be taken to prevent accidental damage, loss or theft of mobile telephone equipment. Any damage, loss or theft must be promptly reported to Information Technology Services.
- Desktop phone diversion to a Bond mobile number is permitted; however, diversion to a personal mobile is to be avoided and requires written permission from the relevant Faculty/Office Business Director. Private use of mobile devices is to be kept to a minimum. Staff may be requested to pay for private calls and data usage on mobile devices.
- Particularly in the case of smartphones, the device may contain trusted or privileged information, and device security is important. In the case of a misplaced device, Information Technology Services should be notified immediately. Blackberry devices connected to the Enterprise Server can be remotely wiped and deactivated.

All call and data bills are paid by Information Technology Services and charged back to the relevant Faculty/Office cost centres.

Bills are monitored by Information Technology Services and if excessive cost is incurred above usual plan caps, the relevant Faculty/Office Business Director is notified to take the matter up with the staff member concerned.

The University, as a responsible employer, has obligations to its employees and as such, will extend a deal of reasonableness and sensitivity toward employees who need to use their Mobile Communications Device for personal use, e.g. in the case of an emergency.

The user is responsible for any and all activities associated with the phone issued to them.

**Risk Management – the Use of Mobile Communications Devices**
This Procedure should be read in conjunction with the Mobile Communications Devices' manufacturer's manual and website.

Staff must not use a hand-held Mobile Communications Device whilst driving a vehicle.

If there are any concerns with a Mobile Communications Device, it can be returned at any time to Information Technology Services. The relevant Faculty/Office will continue to pay the plan costs unless another Faculty/Office assumes responsibility.

**Purchase and Register of Mobile Phones**
Information Technology Services will purchase all Mobile Communications Devices with funds from the relevant Faculty/Office, as needed.

Information Technology Services will ensure that Mobile Communications Devices purchased by the University are capable of performing the duties required.

All fees, charges and call costs incurred by the purchase and use of that Mobile Communications Device will be met by the requesting Faculty/Office.

All Mobile Communications Devices will be purchased outright and remain the property of the University. The University reserves the right to change carriers.

All Mobile Communications Devices will use the University's preferred carrier for voice and data unless there are exceptional circumstances justifying the use of an alternative carrier.

Information Technology Services will maintain a Register of Mobile Communications Devices owned by the University.

Staff may elect to configure personal, privately owned, smartphones to receive Bond email. However, the University will not cover any costs associated with this.

**Equipment Selection**
The University has a List of Preferred ICT Hardware Brands & Models that includes Mobile Communications Devices.

These preferred brands are reviewed from time to time as new products are released and the List is amended on approval by the Vice President Operations.

**Facilities Supported:**
The following phone facilities are supported:

- SMS
- Voicemail
- Connection to computers – cable, infrared, Bluetooth

**Return of Mobile Communications Device on Termination of Employment**
If employment is terminated (by Bond University or employee) the Mobile Communications Device must be returned to Information Technology Services. If the phone is not returned the employee will be charged for the cost of the phone, the SIM card will be disabled, and a fee ($120 + administration) will be charged so that a new SIM can be added to the fleet.

The Faculty/Office should notify Information Technology Services of the redistribution of the phone to another employee in order to update the Register of Mobile Communications Devices.

If the Faculty/Office does not wish to reissue the phone, the Faculty/Office will continue to meet the plan costs unless another Faculty/Office assumes responsibility.

**Dispute Resolution**
Any disputes regarding excessive use above plan caps should be referred to the Head of the relevant Faculty/Office.

**Research Requirement – Discretion of Executive Dean**
Use of Mobile Communications Devices for research projects will be subject to the Executive Dean's approval if the use is outside the scope of this Procedure.

# 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 adhere to the ITS Enterprise Architecture Guiding Principles, located here.

## 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 AND MATRIX**

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 |

# 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.