

 BOND UNIVERSITY	USE OF WIRELESS TECHNOLOGY ON CAMPUS GUIDELINE
Contact Officer	Director, Information Technology Services
Date First Approved	4 October 2004
Approval Authority	Director, Information Technology Services
Date of Next Review	29 May 2026

1. PURPOSE AND OBJECTIVES

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. AUDIENCE AND APPLICATION

All users of Bond University's ICT resources.

3. ROLES AND RESPONSIBILITIES

Role	Responsibility
Director ITS	<ul style="list-style-type: none"> ▪ Approve any variation to these guidelines
All users of wireless infrastructure	<ul style="list-style-type: none"> ▪ Comply with these guidelines and associated Acceptable Use Policies

4. THE GUIDELINE

General Network Access Requirements

Any use of communications technology on the campus, such as Bluetooth, cordless phones, and 802.11 wireless systems, using the standard 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.

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.

Additional Guidelines

- a) Bond reserves the right to use the following 802.11 protocols on campus to deliver wireless services to staff and students:
 - 802.11a/b/g/n/ac/ax/be and future Wi-Fi Alliance standards operating at standardised frequencies;
- b) Users of Wireless Technology must adhere to the [ACMA LIPD](#) licence stipulations for short-range devices.
- d) Devices must not interfere with Bond services including, but not limited, to Wi-Fi, audio-visual, IOT or building management systems. If interfering Wireless Technology is found to be in use, the owners will be required to cease its use.
- e) Unauthorised installation of 802.11 and non LIPD systems are not permitted.

- f) 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.

6. RELATED DOCUMENTS

[ICT Acceptable Use Policy INF 6.1.11](#)

7. MODIFICATION HISTORY

Date	Sections	Source	Details
29 May 2023			V2
19 November 2019			