Wireless Access Policy

Section 1 - Overview

(1) The UNE Information Technology Directorate (ITD) is responsible for the management and operation of the UNE campus information technology (IT) network infrastructure, both fixed and wireless. Wireless networking provides many benefits to the University community in the pursuit of its primary learning, teaching and research objectives. This policy is intended to protect the reliability and security of the UNE wireless network and ensure its inter-operability with the rest of the UNE network.

Section 2 - Scope

(2) This policy applies to all users of the University's wireless network, including UNE representatives and students (as defined at the conclusion of this policy).

Section 3 - Policy

(3) The Information Technology Directorate is the sole body responsible for providing wireless access points connected to the UNE fixed network.

(4) The Information Technology Directorate will routinely monitor the wireless network to ensure that no unapproved access points are present. Access to and use of the UNE wireless network will only be granted upon approval by the ITD. Approval will be contingent upon the user providing evidence of the following:

a. Valid personal authentication credentials;
b. That any devices to be used or installed will be
    i. fully patched;
    ii. running up-to-date virus protection software where available;
    iii. compliant with WPA2 cryptography protocol (or better) and appropriate Australian communications regulations and standards;
    iv. operated so as not to cause interference or disruption to the UNE wireless network or other wireless users. Any device or equipment found to be interfering with or disrupting the UNE wireless network may be subject to a request for relocation or removal.

(5) Installation of wireless access points is forbidden unless ITD have specifically approved the installation

(6) Authorisation to add an access point to the network must be obtained as specified in the Information and Communications Infrastructure Policy.

(7) Unauthorised interception of UNE wireless network signals is prohibited.

(8) Authorisation to intercept the wireless network must be obtained in writing from the Director, Information Technology, by presenting a case in writing that explains the rationale for the interception and precautionary activities to ensure data gathered, must be stored and used appropriately in accordance with relevant privacy law and

legislative documentation.

(9) "Wifi Protected Setup" features must not be enabled on any UNE wireless access point.

(10) All use of the UNE wireless network is subject to the Rules for the Use of Information and Communications Facilities and Services.

(11) The user is responsible for ensuring any wireless device used to access University data and services meets appropriate security and reliability standards.

(12) Policy Compliance

a. All UNE representatives, UNE students (see definitions below) and users of the UNE wireless network within the scope of this policy, must comply with the above policy statements. Failure to do so will be perceived as misconduct and will be addressed via the appropriate misconduct procedures for UNE staff or students.

Section 4 - Definitions

(13) Student - means an admitted student or an enrolled student, at the relevant time.

a. Admitted student - means a student who has been admitted to a UNE course of study and who is entitled to enrol in a unit of study.
b. Enrolled student - means a student who has been admitted to a course of study at UNE or elsewhere and who is enrolled in a unit at UNE.

(14) UNE representative - means a University employee (casual, fixed term or permanent), contractor, agent, appointee, UNE Council member or any other person engaged by the University to undertake some activity for or on behalf of the University. It includes corporations, incorporated bodies of the University and other bodies falling into one or more of these categories.

(15) UNE wireless network - means a telecommunications network that relies upon radio waves instead of copper or fibre optic cable, in the delivery and receipt of information signals. In a wireless network, a device transmits a radio signal through an antenna.

(16) Wi-fi Protected Setup(WPS) features - developed by the Wi-Fi Alliance http://www.wi-fi-org with a view to standardising and simplifying set up and security on wireless networks.

(17) Wireless access point (WAP) - is a device that connects wireless devices (by their radio waves) to a wired network. The access point normally connects to a wired Ethernet connection, and then provides wireless connections for other devices in the area (eg. Wireless routers). WPA2 -Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) - are two security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks.

Status and Details

Status	Historic
Effective Date	27th July 2015
Review Date	14th January 2015
Approval Authority	Vice-Chancellor and Chief Executive Officer
Approval Date	4th November 2013
Expiry Date	6th June 2017
Unit Head	Angie Hendrick Chief Information Officer 02 6773 2044
Author	Robert Irving Chief Information Officer
Enquiries Contact	Technology and Digital Services +61 2 6773 5000