

# University of New England

## Personal Mobile Computing Guidelines

### Document data:

<b>Document type:</b>	Policy
<b>Administering entity:</b>	ITD
<b>Records management system number:</b>	D11/30644
<b>Date approved:</b>	<b>14 November 2011</b>
<b>Approved by:</b>	Vice-Chancellor
<b>Indicative time for review:</b>	3 years
<b>Responsibility for review:</b>	ITD
<b>Related policies or other documents:</b>	UNE Risk Management Policy, Rules for the Use of Information and Communications Facilities and Services, IT Security Policy Audit Vulnerability Scan Policy, IT Security Objectives and Framework, General Server Security Policy, General Password Policy, P2P File Sharing Policy, Personal Mobile Computing Policy, Standards and Guidelines for all Users of University Computing and Network Facilities, Standards and Guidelines for Desktop Computers, Standards and Guidelines for Non-Strategic Systems, Standards and Guidelines for Strategic Systems

### 1. Rationale and Scope

The advent of cheap mobile computing devices has increased the ownership of them among staff and students. The Information Technology Directorate (ITD) has had increased requests for these devices to be connected to the UNE network. ITD acknowledges an obligation to ensure appropriate security on the UNE network and to regulate the use of these devices.

This Document defines the security required for personal mobile computing devices such as laptops, tablet computers and other types of mobile devices that can connect to the wired network or Local Area Network (LAN). Wireless network connections are not part of this policy.

### 2. Policy

#### 2.1. Connecting personal laptops

- To connect a personal laptop to the UNE network, the laptop will require registration with IT Support section of ITD.

## 2.2. Conditions of use

ITD will allow staff or students (hereafter referred to as "the client") to connect their own personal laptop to the UNE Network under the following circumstances/conditions:

- The client is aware of their obligations under the “Computer and Internet Acceptable Use Policy”, “IT security policies” and other related University policies such as the UNE Code of Conduct for Staff;
- Personal devices, if capable, will have virus-checking installed, operating and loaded with current virus updates;
- The client is responsible for ensuring the device operating system has had all relevant security patches applied;
- The client is responsible for purchasing and using licensed software on their device. Some software at UNE cannot be licensed for use on personal devices. Please check with the IT Service Desk for software licensing;
- The client’s device must meet the supported operating system specifications as set by ITD. The it-services section of the UNE website specifies the valid specifications.
- Permission to connect to the network can be withdrawn at any time should any of the above conditions not be met.

## 2.3. Using a personal mobile computing device at UNE

Many staff and students choose to bring personal mobile computing devices onto campus at UNE. It is important for such staff and students to assume responsibility for the safe configuration of their device in order to protect themselves and the University from security breaches.

ITD suggests that individuals:

- Ensure that all operating systems on the computer are promptly patched when the vendor releases relevant patches. Windows users can check for updates using Internet Explorer, and clicking on Tools, then clicking on Windows Update;
- Ensure that software applications used on the computer are promptly patched when the vendors release relevant patches. Most vendors have an email subscription service to notify users of updates, or a software setting to check for updates;
- Maintain a cautious approach to the configuration of applications and do not enable sharing of files and new modes of communication without advice on how to manage these securely;
- Ensure that reputable anti-virus software is actively protecting your computer, and regularly updating its effectiveness;

- Consider using a personal firewall to protect your computer from unwanted network connections – or if using broadband services at home consider using a broadband modem and firewall device that can be configured to assist this; and,
- Comply with all IT related policies.

### **3. Enforcement**

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

### **Approval signature**

Vice-Chancellor