Wireless & Bluetooth Policy

1 INTRODUCTION

Whilst the University expects its employees and staff to comply with this policy, it does not confer contractual rights or form part of any contract of employment and may be amended by the University or replaced at any time following appropriate consultation and negotiation with recognised trade unions. Breach of this policy may be addressed via the University's Disciplinary Policy and Procedure and Code of Conduct.

This policy will be reviewed by the IT Services and Human Resources department on a 3-year basis or amended in response to changes in future legislation and/or case law.

2 OWNERSHIP

The IT Services and Human Resources department owns and manages this policy on behalf of The University of Northampton.

3 ORGANISATIONAL SCOPE

This Wireless & Bluetooth policy is a corporate policy and applies to all employees (and workers, as applicable) of The University of Northampton including any wholly owned subsidiaries, unless an alternative policy exists, subject to any qualifying conditions.

4 POLICY STATEMENT

4.1 Misconfigured wireless (WiFi) networks and vulnerabilities in wireless legacy encryption and authentication protocols continue to be targeted by malicious individuals who can exploit these vulnerabilities to gain access to internal networks. Due to the inherent properties of WiFi (i.e. no physical connection required), they can sit outside a building and with little restriction on time and resources, try to break into a network through a WiFi access point.

4.2 Bluetooth connections are vulnerable to interception along with any data communicated. In addition to the risk of other people being able to receive information, they can also send files or viruses.

5 DEFINITIONS

Wifi
A wireless networking technology that allows computers, smartphones or other devices to communicate over a wireless signal within an area.

Bluetooth
An open wireless technology standard for transmitting fixed and mobile electronic device data over short distances

WPA2
Wi-Fi Protected Access II (WPA2) is a security standard to secure computers connected to a Wi-Fi network.

Generic account
An account that is shared or is not tied to one specific user.

Wifi scanner
A device used to scan an environment for rogue, unauthorised and insecure WiFi access points, in order to maintain a secure network connection.

Firmware
A software program or set of instructions programmed on a hardware device. It provides the necessary instructions for how the device communicates with the other computer hardware.

Hidden-mode
Prevention of other Bluetooth devices from recognizing your device.

SNMP Community String

A user id or password that allows access to a router's or other device's statistics**.**

6 KEY PRINCIPLES

6.1 The controls to protect University of Northampton's WiFi networks are:

- WiFi access points should be situated in controlled areas or situated so that they restrict physical access where practical.
- All WiFi access points connected to the University's internal network shall only allow access via the University's logging in process. There will be no generic or shared passwords/accounts allowable and authentications shall by using WPA2 encryption or higher.
- Users shall not setup their own WiFi access points within the University's environment that could allow access to the University's internal network.
- All WiFi access points must be installed and maintained by IT Services and an inventory kept of each access point, it's use and its user base.
- IT Services will on a regular basis (at least quarterly) use WiFi scanners to identify and remove rogue access points.
- IT Services will ensure that all WiFi access points connected to the University's internal infrastructure, will have default wireless encryption keys, passwords, and SNMP community strings, changed to a secure standard as defined by the Password Protocol and the IT Services System Hardening and Configuration Policy.
- IT Services will ensure that all devices that support the University of Northampton's internal WiFi will be secured in line with the manufacturer's/vendor's recommendations as per the System Hardening and configuration policy. Should new threats come to light, the IT Service should liaise with the manufacturer or vendor to ascertain whether firmware updates or changes in configuration settings are required.

6.2 Bluetooth security requirements are:

- Users should not use Bluetooth connectivity to send or receive information
- If using a Bluetooth device (such as a headset), ensure the default pin is altered (required to pair the device).

- Switch off a Bluetooth headset when it is not in use.
- By default, where a Bluetooth device has been configured by IT Services the device shall use the hidden-mode (non-discoverable).

To protect the University of Northampton's network further, users must ensure the following behaviours:

- Switch off the Bluetooth connectivity on a mobile device when it is not in use.
- Ensure the mobile device has a secure lock screen.
- Ensure the mobile device runs all security updates, supplied from the device manufacturer.
- Do not leave mobile phone unattended.
- If the mobile screen unexpectedly turns on, look and see why. A key flaw in the Bluetooth exploit is that it will turn on your screen if an attacker attempts to do something once connected.
- If you suspect your UoN mobile device has a Bluetooth vulnerability, report it to IT Services.

7 PROCEDURE

7.1 Disabling Bluetooth Connectivity

a) Locate 'Settings' on the device
b) Locate 'Connections' section
c) To the right of 'Bluetooth' label is a toggle button. If off, the button will appear grey. If on, tap to disable.

7.2 Bluetooth Hidden Mode

a) Locate 'Settings' on the device
b) Locate 'Connections' section
c) Found beneath the 'Bluetooth' toggle button, is 'Phone visibility'.
d) Select the toggle button – if already in hidden mode, the button will appear grey. If blue, tap the button to put in hidden mode.

In event you need to use the Bluetooth function, you will need to enable the phone visibility option also.

7.3 **Security Updates**

To enable security updates, ensure your mobile device is regularly turned on and connected to secure Wifi or mobile internet. Updates will be installed automatically – notification may occur.

7.4 **Enabling lock screen**

a) Locate 'Settings' on the device.
b) Locate the 'Lock screen and security'.
c) Select 'Screen lock type'. Select preferred method: pattern, pin or password.
d) Create a pattern / pin or password.

8 ASSOCIATED DOCUMENTS

Remote Access & VPN Policy
Acceptable Use Policy
BYOD Policy

9 EQUALITY IMPACT ASSESSMENT

An Equality Impact Assessment has been completed with this document.

10 VERSION CONTROL

Version Control	1.0	**Approval record**	
Author:	IT Services	Approval:	TU Liaison – 18/09/2018 UMT – 09/10/2018 Boar – 11/12/2018
Date written:	August 2018		
Current status:	Live		