Ulster University Standard Cover Sheet

Document Title	WIRELESS NETWORKS STANDARD 4.4
Custodian	Head of Infrastructure
Approving Committee	ISD Committee
Policy approved date	2017 – 08 – 10
Policy effective from date	2017 – 08 – 10
Policy review date	2018 – 08 – 10

Changes to previous version
Page 3 – Change “that they are in compliance with to “compliance”.

INTRODUCTION AND BACKGROUND

The University's wireless networks have become an important and integral part of University business processes, and also in the delivery of teaching and research. This document defines how wireless technologies are to be deployed, administered and supported. The implementation of this standard will assure that all constituents using wireless communication networks receive an acceptable baseline level of service quality with respect to reliability, integrity, availability and security.

Further information on ISD policies, standards and guidelines is available at:

http://www.ulster.ac.uk/isd/policies

RELEVANT LEGISLATION

The University will comply with all legislation and statutory requirements relevant to information and information systems, including:

- Computer Misuse Act 1990;
- Data Protection Act 1998;
- Communications Act 2003;
- Copyright, Designs and Patents Act 1988;
- Freedom of Information Act 2000;
- Human Rights Act 2000;
- Regulation of Investigatory Powers Act 2000;
- Police and Justice Act 2006;
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 ('the Lawful Business Regulations')

STANDARD

Information Services (ISD) Service Provision

- ISD shall deploy all University Wireless Access Points.
- To protect the integrity of the University network infrastructure and prevent unauthorised access, all open wireless access areas will be connected to a separate wireless VLAN through a gateway service which will be used to permit or deny access to the University network.
- To be granted access to the University network wireless clients will have to authenticate at the wireless gateway. Authentication and authorisation will be based on University approved user accounts and JANET eduroam visitor accounts.
- Following authentication, a limited range of supported applications will be permitted.
- ISD will manage and monitor the usage of the wireless network.

- ISD will monitor the development of wireless network technology, evaluating wireless network technology enhancements and as appropriate incorporate new wireless network technology within the University network infrastructure to meet business and security requirements.

Departmental and Third Party Wireless Networks

- Departments who wish to provide a wireless service should in the first instance discuss their requirements with a member of the ISD network team.
- Only wireless access points provide by ISD can be connected to the University network. For departments that require their own Wireless service, ISD will broadcast their SSID over the existing University Wireless Infrastructure.
- Where a departmental or third party wireless access point interferes with a central service provision or prevents campus wireless provision in that area, then the departmental or third party must defer to the centrally provided one if a workable solution is not available.

Security

Wireless networks are inherently less secure than wired networks. Because the signal is broadcast the wireless network is shared and any wireless device can listen to network traffic from any other wireless device that is in range. Without using any application to support security and privacy, the wireless network must be regarded as being open and not secure.

- Unless using encrypted protocols on secure Wireless Access Points, wireless clients must not be used for connecting to UU business systems such as Human Resources, payroll, student information, financial information, or other systems that transmit sensitively classified (PROTECT or CONTROL) information or that are critical to the mission of the University.
- Staff must not use wireless access in areas for accessing or transmitting unencrypted sensitive or confidential information. Access to unencrypted sensitively classified (PROTECT or CONTROL) information should only be from secure wired network connections.
- Under no circumstances is a user to share their authentication credentials with others through facilities like Microsoft WiFi Sense.

User Requirements

- Under no circumstances is a staff member or student permitted to connect any form of Wireless Access Point to the University Network.
- Users should note that they are responsible for:
    - Ensuring their wireless device has up-to-date patches, anti-virus software, personal firewall and other measures to protect it whilst operating on an insecure network;
    - Any equipment that is connected to their system, for ensuring that it is in good working condition and that it will not present a health and safety risk to them, others or University property;
    - Ensuring their wireless device is virus free.

- Users should be aware that:

    - Use of a wireless LAN connection in “”ad hoc”, “hot spot” or “tethered” mode is unacceptable, as it may interfere with legitimate wireless networks elsewhere on campus. Wireless devices discovered not in infrastructure mode may be disconnected from the network and/or users will have their user account disabled;
    - If found to be using a wireless LAN connection that is consuming high bandwidth, which contributes to a deterioration of the wireless network, it may be disconnected from the network and/or have their user account disabled;
    - That the wireless network is not secure;
    - Use of the University wireless network implies compliance with the University Acceptable Use Code of Practice;
    - The University will not accept responsibility or liability for any damage to or loss of data to their portable device while in transit or connected to the University network;
    - That activity on the University network will be monitored and recorded to secure effective operation, and for other lawful purposes.

PURPOSE AND SCOPE

The purpose of this standard is to define how wireless technologies are to be deployed, administered and supported at the Ulster University. The implementation of this standard assures that all constituents using wireless communication networks receive an acceptable baseline level of service quality with respect to reliability, integrity, availability and security.

IMPLEMENTATION AND ENFORCEMENT

- Connection of an unauthorised Wireless Access Point to the University network is prohibited. Efficient operation of wireless networks depends on a planned approach to the allocation of the limited spectrum available. Rogue Wireless Access Points (any Wireless Access Point not registered with ISD) jeopardise the integrity of the wireless infrastructure and may interfere with and degrade the performance of authorised services. Surveying and monitoring will be undertaken to locate Rogue Wireless Access Points and any found will be disconnected from the network.
- In the event of any abuse of facilities, ISD reserves the right to withdraw access until the matter has been dealt with by the appropriate authority.