Wireless Service

Policy and Procedure

Document Control

Date	Revision/Amendment Details & Reason	Author
February 2014	Initial Document	M Beecroft
September 2014	Implementation of eduroam	M Beecroft
25th November 2014	Approved by University Council	

1. Introduction

The purpose of this policy is to ensure that the deployment of the wireless network is controlled and managed in a centralised way to provide functionality and optimum levels of service whilst maintaining network security.

The intention of this policy is to define roles and responsibilities for the design of any wireless network, the installation, registration and management of wireless access points, adequate management and allocation of the wireless frequency spectrum and the services offered to end users for wireless access.

The policy is maintained and regulated by the University's IT Services department.

The policy is cross-referenced to the University IT policies and external policies such as the JANET eduroam policy. Copies of these policies can be found on the IT Services section of the University website.

2. Background

In the process of implementing a Wireless network service, there are three issues which need to be addressed viz

- **Interference**

  802.11 wireless technology uses frequencies from a band which is divided into channels. In order for adjacent access points to work with each other and not cause interference, a different channel must be used for each Access Point (AP). Although there are multiple channels within the band, only three are non overlapping and can guarantee a signal free from interference. It is therefore required that the appropriate channel is assigned to the AP dynamically by the wireless controller in order to avoid any interference related performance issues.

- **Security Problems**

  Wireless LANs offer connectivity to anyone within range of an access point; physical boundaries are no longer a relevant option for preventing access to the network. Installation of non-approved devices with little or no security which, if connected to the University network, would breach the security of the main infrastructure allowing any unauthorised user with appropriate equipment to connect.

- **Danger of Device Diversity**

  Non-standard or misconfigured wireless devices can cause disruptions to the wireless LANs and subsequently the wired network. IT Services prohibits the installation of any non-standard wireless access points. The policy is to centralise the purchase and installation of wireless equipment to ensure that inappropriate devices are not installed and used on the University network.

This policy outlines a common set of procedures and operational criteria, in order to effectively manage 802.11 wireless LANs. It covers the ways in which these three issues have been addressed to the required standard.

The policy also describes the standards that users are expected to observe when using University wireless facilities, and ensures that users are aware of the consequences of inappropriate use of the facilities.

Finally, the policy specifies the actions that the University will take in the investigation of complaints received from both internal and external sources, about any unacceptable use of University wireless facilities.

3. Policy Statement

Scope of the Policy

This wireless policy applies to all areas of wireless connectivity to the University network infrastructure on any of the University premises, or any remote location directly connected to the campus network. IT Services has the sole responsibility for the design, deployment and management of the University wireless LANs.

Technical Requirements

The wireless infrastructure will comply with the following requirements:-

- All Access Points will abide by all national regulations relating to Wireless Devices.
- All existing Access Points must conform to recommended specifications as defined by IT Services.
- All new Access Points will be purchased by IT Services.
- All Access Points will utilise the IT Services approved configuration settings.
- Access Points will only support the 802.11b, 802.11g and 802.11n standards.

- Allocation of channels, SSID and encryption standards will be performed by IT Services

- All wireless LAN communications will be encrypted

- All wireless communication will require user authentication before granting access to the network

- Any future request for installation of new Access Points must be directed through IT Services.

- IT Services acts as the central management body in regulating the installation and maintenance of all 802.11 wireless LANs.

Monitoring

- IT Services prohibit the installation of any non-standard Access points.

- In line with the IT Acceptable Use Policy, IT Services has the right to disable any non-standard device which may cause interference with existing approved Access Points. The offending device may be removed without prior notice.

- Monitoring of wireless networks is undertaken by IT Services on a regular basis and any unauthorised wireless equipment will be removed from the network.

Acceptance of Policies and Regulations

It is a condition of the use of IT facilities provided by the University, that the user agrees to be bound by the relevant University Policies and Regulations.

4. Installation and Management

Proper installation and management is critical for a successful wireless LAN deployment. The following criteria must be followed:

- There are no restrictions on installation or placement of equipment in force for the proposed location. If required, advice should be sought from Estates

- A site survey is carried out prior to installation to ensure:

    - No interference to/from other radio sources

- Optimum location for desired coverage including connections to power and 'wired' network connection point

- Installations must comply with all health and safety, building and fire regulations
- Access Point configuration and client access conforms with this policy and all other University IT Policies
- Deployments are fully maintained and supported commensurate with this policy
- Installation and support staff with appropriate skill levels are identified together with their roles and responsibilities

5. Security and Access Controls

Security provisions must be inherent in the design and implementation of all wireless LAN deployment. Security provisions must provide adequate measures to guard against unauthorised access to or miss-use of University provided IT resources; in particular measures must be implemented to ensure:

- User authentication and authorisation credentials are established before access to resources are permitted
- Access to the service will be restricted to authorised staff and students via membership of a User Group. Adding and deleting of users into the group is contained within the document "Process for setting up and deleting users on the Wireless service"
- Strong data encryption procedures are implemented on the Wireless LAN before access to resources are permitted
- Support staff and monitoring tools are available to help investigate incidents and ensure compliance with this and other relevant University policies
- All relevant associations are recorded i.e.
    - Wireless client with access point, including time stamps
    - Wireless client/user authentication status, including time stamps
    - Wireless client MAC address and assigned IP address, including time stamps

- Only those servers and services necessary for the legitimate operation of the wireless LAN are connected
- Stations operating in Ad-Hoc mode are not permitted
- Stations offering services that compromise security e.g., Proxy, relaying, routing, or BootP/DHCP services are not permitted
- Stations in breach of this Policy or any other relevant University Policy can be identified and if necessary removed or blocked from accessing the wireless LAN
- Implementing the 802.1x standard for initial authentication and authorisation together with strong WPA2 – AES encryption and radius policy based VLAN restrictions

6. Roles and Responsibilities

IT Services will be responsible for:

- Policy maintenance and updates
- Recording and reviewing wireless LAN registrations
- Monitoring wireless LAN compliance with this and other University Policies
- Resolving interference problems
- Designing, deploying, supporting and managing wireless LANs in common flexible access areas
- Designing, deploying, supporting and managing wireless LANs that require connection to the University's campus network
- Recording associations i.e.
    - Wireless client and access point associations, including time stamps
    - Wireless client/user authentication status, including time stamps
    - Wireless client MAC address and assigned IP address, including time stamps
- Monitoring and recommending wireless LAN standards for use on campus
- Ensuring other authorised providers understand the support and security overheads associated with wireless LAN deployments

- Informing users of all Policies relating to the use of wireless LANs
- Providing assistance to other authorised providers in the design and deployment of wireless LANs

Users will be responsible for:

- Adhering to this and all relevant University Policies
- Providing, registering, configuring and maintaining their own systems for use on the flexible access wireless LAN
- Users of the wireless network are responsible for their own computer equipment. The University accepts no responsibility for any loss or damage to their machine as a result of connection to the wireless network.
- Users have the responsibility to ensure that they are running up to date antivirus software and that the operating system is fully patched with the latest service packs and hot fixes.

7. Policy Review

This policy will be reviewed on an annual basis with particular regard to the expected developments in wireless technology and operational use within the University, and by reference to the development of recognised best practice.