WIRELESS ACCESS

POLICY DOCUMENT

Document Id	Wireless Access Policy
Sponsor	Laura Gibbs
Author	Nigel Rata and Frank Madden
Date	May 2014

Version Control Log

Version	Date	Change
1.0	15/05/12	Initial draft for review
1.1	15/05/14	Annual Review

Document Approval

Name	Approval Signature	Approval Date
ITUAG	Approved	27.5.14

Purpose

The University's wireless networks have become an important and integral part of University's delivery of teaching and research and many business processes. This policy describes how wireless technologies are to be deployed, administered and supported at Royal Holloway University. The implementation of this policy assures that all constituents using wireless communication networks receive a reasonable level of service quality with respect to reliability, integrity, availability and security

RHUL Wireless Provision

- Royal Holloway University 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 VLANs 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/guest accounts.
- Following authentication a range of supported applications will be permitted, some services may be blocked due to unsuitability for wireless connectivity (e.g. multicast TV channels or other multicast services).
- All wireless access points at the university should be centrally provided.
- Royal Holloway University will manage and monitor the usage of the wireless network as it does the wired network.
- The Royal Holloway centrally managed wireless network solution operates real time RF space management, all other wireless devices on Campus will be subject to this control.
- Royal Holloway University will monitor the development of wireless network technology, evaluating wireless network technology enhancements and as appropriate

include new wireless network technology within the University network infrastructure to meet business and security requirements.

Departmental Wireless Networks

The Royal Holloway University wireless network provides coverage to nearly 100% of internal building spaces on Campus and remote sites. In the rare case that Departments wish to install wireless access points, they should in the first instance discuss their requirements with a member of the IT Network team. Wireless access points must be registered with IT Services and use only the wireless channels and IP addresses allocated by IT.

The radio frequency space is congested and therefore permission must be sought from IT before access points are installed within departments that are not part of the centrally managed solution.

Where a department is permitted to install a new wireless access point to support its teaching and research purposes, firstly the access point must be purchased through IT services and secondly security on such a network is the responsibility of the department concerned. At a minimum it should:

- Authenticate all user access, ensuring that only known staff members have access. Access point **must not** be open to guests, unauthorised and unauthenticated users.
- The system must only allow known specified MAC addresses to join the network.
- Be able to identify users in cases of reported misuse.
- Change the default wireless channel.
- Ensure the access point is connected to a dedicated Ethernet switch port.

Where a departmental wireless access point interferes with a central service provision or prevents campus wireless provision in that area, then the departmental network must defer to the centrally provided service if a workable solution is not available. This also applies to other devices using the radio spectrum such as cordless telephones.

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.

At Royal Holloway University we have chosen not to encrypt our wireless traffic and use application encryption instead (such as HTTPS or SSH).

Wireless Services

Royal Holloway University provide 2 standard network services over all centrally managed wireless access points:

- CampusNet – this is the primary RHUL service for wireless users to get RHUL network access. Users must authenticate with a valid college username and password to gain access to this system. The CampusNet service is protected by an internal firewall.
- Eduroam - (education roaming) is a secure international roaming service for users in Higher Education. The European Eduroam confederation (a confederation of autonomous roaming services) is based on a set of defined organisational and technical requirements that each member of the confederation must agree to. It is designed to allow for visiting users from participating universities and affiliated institutions to authenticate and receive internet services at other participating institutions.

In addition, additional wireless networks may be presented in some or all of the site/s. These relate to specific projects or events and will deliver services appropriate for the situation. Any additional wireless SSIDs and associated network transit configuration must be authorised by the IT Infrastructure manager.

Requests for specific additional permanent or temporary Wireless networks to be broadcast on the RHUL Wireless service by customers outside of IT should be made via e-mail to itservicedesk@rhul.ac.uk.

User Requirements

- Under no circumstances is any student permitted to connect any form of Wireless Access Point to the University Network.
- Users should note that they are responsible for:
  - Ensuring their Laptop 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 Laptop is virus free.
- Users should be aware that:
  - Use of a wireless LAN connection in “ad hoc” mode is unacceptable, as it may interfere with legitimate wireless networks elsewhere on campus. Laptops 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 that they are in agreement with the University Acceptable Use Policy;
  - The University will not accept responsibility or liability for any damage to or loss of data to their machine while in transit or connected to the University network;

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 RHUL) jeopardises the integrity of the wireless infrastructure and may interfere with and degrade the performance of authorised services. Surveying and monitoring may be undertaken to locate Rogue Wireless Access Points and any found will be disconnected from the network.

This policy will be reviewed annually.