LIVERPOOL HOPE UNIVERSITY
Est. 1844

Wireless Service

Protocol

Document Control

Responsibility for Document:	Chief Information Officer
Approved by and date:	USET 31st October 2023
Frequency of Review:	Annual
Next Review date:	November 2024
Related Policies:	IT Facilities Acceptable Use Policy Information Security Policy
Minor Revisions:	

LIVERPOOL HOPE UNIVERSITY
Est. 1844

1. Background

The University Wi-Fi service is provided by IT Services who:

- has the sole responsibility for its design, deployment and management
- acts as the central management body in regulating the installation and maintenance of all wireless networks
- procures and installs all wireless infrastructure equipment.

The main Wi-fi network broadcast is eduroam (although there are others that are provided for defined specialist usage) that supports the following standards:

Generation	IEEE Standard	Adopted
Wi-Fi 7	802.11be	(2024)
Wi-Fi 6E	802.11ax	2020
Wi-Fi 6	802.11ax	2019
Wi-Fi 5	802.11ac	2014

Devices using earlier standards may work on the University network but this cannot be guaranteed.

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

2. Challenges

There are two main challenges in providing a Wi-Fi service viz

Performance

Wireless technology uses frequencies from a band which is divided into channels. For the service to run effectively and without interference, each broadcasting device must use a different channel. The University service is provided by approximately 1,000 broadcasting devices with the channel assigned from central, University controlled equipment.

The service can be disrupted by the introduction of non-University provided equipment that may use the same channels as the University devices. In some case, such disruption can also impact on the University wired network.

Security

Wi-Fi networks and devices are targeted by malicious players who can exploit vulnerabilities to gain access to internal networks and data. Due to the inherent properties of Wi-Fi (i.e. no physical connection required), these players can sit outside a building and, with little restriction on time and resources, try to break into a network.

Such vulnerabilities can exist in all wireless data communication devices (e.g., personal computers, mobile phones, hand-held devices, routers from rooms in halls etc.) connected to any of the University's network infrastructure devices. This includes any form of wireless communication device capable of transmitting / receiving data.

Installation of non-approved devices with little or no security could, if connected to the University network, breach the security of the main infrastructure.

3. User Responsibilities

Whilst IT Services will take appropriate measures to mitigate the risks to the University Wi-Fi service provision, users of the service (both staff, students and visitors) will be required to:

- refrain from installing onto the University IT networks any personal network devices including but not restricted to:
    - personal and domestic routers
    - personal firewall devices
    - personal portable routers (mobile hotspot devices)
    - personal switches and repeaters
    - personal wireless access points or repeaters
    - laptops or PCs set up to provide Internet Connection Sharing or its equivalent

  Wireless printers may be used if connected via a USB port and the wireless functionality switched off
- 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
- ensure that they do not provide access to the network to other users (for example by connecting a hub or modem to a networked computer)

- be responsible for their own computer equipment. The University accepts no responsibility for any loss or damage to their devices as a result of connection to the wireless (or wired) network.
- utilise the service in an appropriate manner including but not restricted to:
    - authenticating on to the wireless network for each session only with their own credentials
    - be responsible for all activity on their devices
    - be bound by the relevant University Policies and Regulations.

4. Monitoring of the service

Log files are generated from the service including:

- recording wireless network registrations
- monitoring wireless network compliance with this protocol and other University Policies
- designing, deploying, supporting and managing wireless networks that require connection to the University's campus network
- recording access data

If and when identified, IT Services has the right to disable or remove, without prior notice, any unauthorised wireless equipment that may impact on the service or represent an unacceptable security risk.

5. Protocol Review

This protocol 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.