Wireless Networking Policy

Contents

Introduction

This policy document relates specifically to wireless networking at Newman University and should be read in conjunction with the General Conditions of Use of Computing and Network Facilities.

The Wireless Network Policy applies to all wireless network users (staff, students, visitors) and equipment operating within the University. The wireless network will run in parallel with the wired University Network and aims to satisfy the needs of users who require mobility and flexibility in terms of their working locations.

In order to limit the potential security risks that may be associated with wireless network technologies, access to the Wireless Network must take place in a controlled and secure manner.

IT Services will make a reasonable effort to connect your equipment to the Wireless Network; however we do not guarantee a connection. A judgement on reasonable effort will be made by a member of IT services, and will be dependent on resources that are available to them.

IT Services will continue to monitor, evaluate, develop and where applicable, incorporate new wireless network technology to the benefit of the University community.

Breach of Wireless Network Policy directives will result in immediate action being taken to disconnect any unapproved networking equipment and in the case of deliberate or repeated abuse may be treated as a disciplinary offence.

Authority and Responsibility

IT Services is responsible for authorising, managing and auditing connections to the University Network, as well as for the security and integrity of the Network. Records and logs are kept providing audit data for the purpose of tracking connectivity issues and possible misuse.

As part of this remit, IT Services is responsible for producing and maintaining the Wireless Networking Policy and for establishing standards for the deployment of wireless network technology.

IT Services is also responsible for managing the University Wireless Network spectrum, given the potential for co-channel and adjacent-channel interference from competing wireless network devices within a given location.

No wireless installations are allowed without IT Services' authorisation.

Anyone needing to install a wireless network or device should contact IT Services for advice about how their requirements might be met through or alongside the Wireless Network. All such queries should be referred to the IT Helpdesk (support@newman.ac.uk)

Any queries, comments or suggestions relating to the Wireless Networking Policy should be directed to the Director, IT Services, or to the Network Team wireless@newman.ac.uk

Design

The Wireless Network is separated from the wired network by a dedicated firewall. In order to provide more robust security and to observe good practice the Wireless Network has dedicated switching and cabling infrastructure and as such is maintained independently of the wired network, including independent IP addressing.

The Wireless Network is presently based upon the 802.11a/g/n standards operating within the unlicensed 2.4GHz frequency range for 802.11a/g/n at 11Mbps and 54Mbps, and 802.11n (5GHz) at 450Mbps.

Access and Availability

All Staff and Students who are currently registered on the IT Services Active Directory will automatically be granted access to log on (Authenticate) to the wireless network using their normal login and password credentials. Instructions detailing access and configuration can be found on the main Wireless Webpages located at: https://sharepoint.newman.ac.uk/its/its/SitePages/IT Support Help Guides.aspx

Access is switched (time-sliced) based, so each client receives fair access to the available bandwidth.

Wireless Network coverage will continue to expand across the University, operating within the unlicensed 2.4GHz and 5Ghz frequency range, presently:

Standard	Radio Frequency	Speed
802.11a	5 Ghz	54 Mbps
802.11g	2.4 Ghz	54 Mbps
802.11n	2.4 Ghz / 5 Ghz	450 Mbps

IT Services will advertise University Wireless Network Services and associated Service Set Identifiers.

It is expressly forbidden to run unauthorised wireless network devices that utilise the same Service Set Identifiers that are associated with IT Services managed wireless services.

Note: Due to the wide array of devices operating at the same frequencies within the 802.11 2.4GHz range and the subsequent ease of denying service, wireless networks should not be utilised for mission critical applications or services unless absolutely necessary.

Guest Access

Guest access is freely available to visitors, such as contractors, salespeople and other visitors to the campus. Access is provided by the unique 'Newman University Guest' wireless LAN and dedicated fibre connection. Access is available in all public and teaching areas of the campus (excluding Halls of Residence). A password is not required to connect to the service and access is granted with a Facebook, Google+ or Twitter account, or by filling in a registration after connecting.

EduRoam

Eduroam is a secure wireless network service that allows faculty, staff, and students to use their home institution's wireless credentials to access wireless networks when visiting other **Eduroam** participating institutions. The Eduroam wireless provision is primarily for use by visiting colleagues from other institutions.

Authentication and Encryption

The Staff and Student authenticated Wireless Networks currently employ WPA2 as their primary authentication strategy. This provides secure authentication and over the air Advanced Encryption Standard (AES) encryption.

The security for 'Newman University Guest' is much different than security provided for the staff and student WLANs. The main security goal of a Guest WLAN is to provide guests with an easily accessible wireless portal to the Internet while at the same time restricting guest user access from the rest of the company network. The Guest SSID is an open network that has no WPA/WPA2 encryption security. Care should be taken when using the Guest network and users should avoid transmitting sensitive information.

Acceptable Use and Misuse

The University Wireless Network should not be used inappropriately; in particular you should not use the network to:

- send, receive or make available any material that might be considered offensive, obscene or indecent
- send, receive or make available any material that might infringe copyright, e.g. MP3 or other audio and video formats
- run peer-to-peer (P2P) file sharing software, e.g. µTorrent, Vuze, Deluge, Kazaa, Limewire ect..
- intercept or attempt to intercept other wireless transmissions for the purposes of eavesdropping
- access or run utilities or services which might negatively impact on the overall performance of the network or deny access to the network, e.g. RF jamming, Denial of Service (DoS)
- harass, cause annoyance, nuisance or inconvenience to others
- access or attempt to access systems or resources to which you are not authorised
- provide services which may interfere with normal network operation
- provide access to others, e.g. allowing a third party to use your credentials to access the network
- Misuse of the wireless network or University wireless spectrum will be taken extremely seriously. Such misuse may lead to:
- Immediate permanent disconnection of any unapproved wireless networking equipment
- For deliberate or repeated breach of the policy, disciplinary action under current University regulations

Security and Monitoring

Due to possible interference from other sources within the 802.11 wireless 2.4GHz frequency range, the University wireless spectrum should be kept clear of unauthorised transmissions.

IT Services is responsible for maintaining the availability of the University wireless network spectrum. In order to better manage and monitor the wireless spectrum, and to identify rogue devices and possible misuse of the network, IT Services will make periodic sweeps of the University wireless coverage area and in strategic locations, make use of passive monitoring devices and intrusion detection software.

Any unauthorised wireless devices operating within the University wireless spectrum will be considered rogue devices. As such, depending upon configuration, these devices may present a substantial security threat and will be subject to removal from the network.

All wireless installations must comply with the wireless network architecture and standards developed through IT Services.

It is expressly forbidden to connect any wireless network device or equipment directly into the wired campus network.

Wherever possible, wireless access points should be physically secured out of reach or positioned out of sight in ceiling voids (assuming they are plenum rated) for example. Associated switching and cabling infrastructure managed by IT Services will be secured within dedicated wiring closets in accordance with normal practice.

In order to mitigate the clients' exposure to external threat, users' laptop PCs which are used to connect to wireless network must

- utilise a personal firewall
- run anti-virus software and maintain any virus definition updates
- ensure that their operating system is fully patched and running the latest service packs
- not run in ad-hoc mode, i.e. peer-to-peer mode

IT services endeavours to make the Wireless Network universally accessible, we currently do not support all operating systems. For information about supported operating systems, please refer to the IT support guides

If users of the wireless network are in any doubt as to how to maintain their particular client device, assistance can be gained in the first instance through the IT Services Helpdesk, details on the **IT Help Guides** or by visiting the Help Desk in person.

This policy will be reviewed annually.