Wireless Network Acceptable Use Policy

Applicable to all students, faculty, staff and visitors of Harlaxton College

1. Introduction

This policy document relates specifically to wireless networking at Harlaxton College and should be read in conjunction with the **Information Technology (IT) Acceptable Use Policy**.

This Wireless Network Policy applies to all wireless network users (staff, students, faculty and visitors) and wireless network equipment operating within the College.

The wireless network runs in parallel with the College's wired or fixed 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.

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

Breaches of this Wireless Network Policy will result in immediate action being taken to disconnect any unapproved networking equipment and in the case of deliberate or repeated abuse may be subject to disciplinary action.

2. Authority and Responsibility

Harlaxton College is responsible for authorising, managing and auditing connections to the College 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.

Harlaxton College is also responsible for managing the College wireless network spectrum, given the potential for co-channel and adjacent-channel interference from competing wireless network devices within a given location. Therefore, no wireless installations are allowed without the authorisation of Harlaxton College.

Any queries, comments or suggestions relating to this Wireless Networking Policy should be directed to Ian Welsh (**iwelsh@harlaxton.ac.uk**).

3. Design

The wireless network is separated from the wired network by a dedicated firewall and it operates on a different logical network (vlan) to the wired network.

The wireless network is presently based upon the 802.11 a/b/g/n standards operating within the 2.4GHz and 5.2 GHz frequency ranges.

4. Access and Availability

All staff, faculty and students who are registered at Harlaxton College will automatically be granted access to log on (Authenticate) to the wireless network using a personal security key (WPA2-PSK). The security key is unique to the user and may be used on up to three devices (e.g. laptop, tablet, phone).

Wireless access is contention based, meaning that 802.11 wireless networks operate over a shared medium, the performance of which is heavily dependent upon the number of other client connections and their usage.

It is expressly forbidden to run unauthorised wireless network devices that utilise the same Service Set Identifiers (SSID) that are associated with College managed wireless services.

5. Authentication and Encryption

Harlaxton College provides secure wireless connectivity using Wi-Fi Protected Access 2 - Pre-Shared Key (also called WPA or WPA2 Personal) which is a method of securing your network connection using a Pre-Shared Key (PSK) which offers good security/encryption with the convenience of a one-time authentication mechanism

Harlaxton College broadcasts two wireless network options (SSID) for users:

- **Harlaxton (SSID)** - Registered students, faculty and staff will be given a Private-PSK that is unique to them and can be used on up to three devices. This PSK is not shared with other users.
- **Guest (SSID)** – Guest users will be given a Shared-PSK. This PSK is shared with other users and is therefore less secure.

6. Acceptable Use and Misuse

The College 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. Kazaa);
- 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 Harlaxton College 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 College policies.

7. Security and Monitoring

Due to possible interference from other sources within the 802.11 2.4GHz and 5.2 GHz wireless frequency ranges, the College's wireless spectrum should be kept clear of unauthorised transmissions.

Harlaxton College is responsible for maintaining the availability of the College wireless network spectrum. In order to better manage and monitor the wireless spectrum, and to identify rogue devices and possible misuse of the network, the College will make periodic sweeps of the College's wireless coverage area and make use of passive monitoring devices and intrusion detection software.

Any unauthorised wireless devices operating within the College's 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.

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

In order to mitigate users' exposure to external threats, devices which are used to connect to College's wireless network must (where possible):

- 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).

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 itsupport@harlaxton.ac.uk.