Aberdare Community School
Ysgol Gymunedol Aberdâr

Wireless Access Policy

Date Adopted	27th September 2023
Signature of Headteacher	
Signature of Chair of Governors	
Date to be reviewed	September 2025

WIRELESS ACCESS POLICY

Review

This policy has been approved by the Technical Management Team and any amendments to it require the team's approval.

- Last approval: N/A
- Last review: N/A
- Next review: TBA

Overview

It is recognised that wireless networking could offer great benefits to the School community in the pursuit of its primary objectives of learning, teaching and research. Wireless networking has been in existence for a few years, but is still a relatively new technology. The recent ratification of further 802.11 standards for wireless access will continue to enhance interest in the technology. ess network devices utilizing the School IP space including private non-routable IP space within School networks and all users of such devices. It covers all wireless connections to the campus network backbone, frequency allocation, network address assignment, registration in the Domain Name System, and services provided over wireless connections to end users both to and from the campus network.

Computing Services are responsible for the operation and management of campus network infrastructure. A natural extension to the fixed network currently in existence is a wireless network. In order to ensure reliability, integrity and interoperability between the wired and wireless domains it is the responsibility of Computing Services to ensure the design, management and appropriate use of the campus wireless infrastructure is in accordance with best practice and existing policies.

Definitions

Wireless networking is a relatively new technology so some definitions will aid in clarification of the policy.

- Wireless Network: The network technology that uses radio frequency spectrum to connect computing devices to a wired port on the campus network. Common technologies are IEEE 802.11a, 802.11b and 802.11g. Bluetooth is as similar technology.

- Wireless Infrastructure: The wireless access points, antennas, cabling, power, and network hardware associated with the deployment of a wireless network
- Base Station: A network device that serves as a common connection point for devices in a wireless network. Access points use wireless antennas instead of wired ports for access by multiple users of the wireless network. Access points are shared bandwidth devices and are usually connected to the wired network.
- Access point: Same as Base Station.
- Coverage: The physical area where a level of wireless connectivity is available.
- Channel: The chosen frequency for communication between the end point and the base station.
- RF Interference: The degradation of a wireless communication signal caused by electromagnetic radiation from another source. Interference can slow down or eliminate a wireless transmission depending on the strength of the interfering signal.
- Security: The condition that provides for the confidentiality of data transmitted over a wireless network.
- SSID: Service Set Identifier, essentially a name that identifies a wireless network. All devices on a specific wireless network must know the SSID of that network.
- Client hardware/software: The equipment and software that is installed in a desktop, laptop, handheld, portable, or other computing device.

Rationale

There would be three major risks with an ongoing ad-hock deployment of wireless networks in the School.

1. Security: By their very nature wireless LANs are open to anyone within range of the access point. Physical boundaries are no longer relevant. If a wireless access point is connected to the campus network without restrictions anyone with the proper equipment will be able to access the network. Furthermore, anyone with the proper equipment can spy on traffic. They can see users' passwords as well as other data. In line with other policies being introduced in this area security of wireless installations has to be rigorously managed.
2. RF Interference: There is a finite amount of bandwidth available for wireless use. The most common wireless LAN technology (802.11b) defines only 3 (or possibly 4) channels for effective use. If wireless LANs are installed without coordination with others in the area, interference is likely. This may result in significantly degraded performance for everyone.
3. Equipment Diversity: All standards compliant wireless equipment from reputable manufacturers will coexist with each other even leaving aside possible interpretations in the standard. However for a campus wide wireless LAN infrastructure to be properly planned, implemented and managed appropriate hardware needs to be chosen for deployment. Low cost 'consumer-oriented' devices which do not provide the management capabilities for campus wide networks should be avoided in favour of more appropriate equipment.

Roles and Responsibilities

The objective is to define a framework where Computing Services works with departments and faculties to enable the deployment and ongoing management of a wireless network infrastructure. The intention is not to restrict or constrain the growth of the network.

Computing Services shall act as overall coordinators and controllers of the network. Individual departments and IT experts within those departments shall, where appropriate, be responsible for the localised management and implementation of the access points and infrastructure.

The Policy

1. Wireless base stations must abide by all national regulations pertaining to wireless devices. Furthermore base stations shall conform to recommend minimum specifications as defined by Computing Services and other interested parties. Individuals and departments are expected to purchase in line with School purchasing policy and by seeking guidance from Computing Services.
2. No wireless base stations are allowed to be connected to the campus network without prior registration with Computing Services. Wireless equipment is essentially no different to any other network host so must adhere to the Host Connection policy.
3. The locations of and an official point of contact for all wireless access points must be registered with Computing Services. Ideally at least one point of contact will be the official IT supporter for the department who may act as an official representative for a more senior official if that is seen to be required.
4. Allocation of channels, SSID and encryption standards must be agreed and authorised before deployment.
5. ALL wireless LAN communications shall be encrypted.
6. All wireless communication shall require user authentication before granting access to campus network and beyond.
7. Wireless networks must be designed and deployed to avoid any interference between competing devices in the electromagnetic spectrum. Other devices may mean neighbouring wireless base stations or other components using the radio spectrum such as cordless telephones or competing technologies. In the event that a wireless device interferes with other equipment the local department should be expected to resolve the situation. Disputes over channel allocation should be handled by the official point of contact for that base station. Where multiple units or departments are involved Computing Services will act as arbiter or coordinator.
8. Physical security should be considered the joint responsibility of all parties when planning the location of wireless access point and other wireless network components.

Conformance with Existing Policies

Computing Services is authorised to take whatever reasonable steps are necessary to ensure compliance with this, and other network related policies that are designed to protect the integrity and security of the campus network. Specific attention is drawn to the IT Security policy, the Host Connection policy, Computer Systems Monitoring and Scanning policy as well as the regulations and policies outlined below in Related Documentation.

Due to the nature of wireless networks the following addition should also be noted:

Authorisation to disconnect any wireless network on campus network which poses a security threat. If a serious security breach is in process Computing Services may disconnect the LAN immediately. Every reasonable attempt will be made beforehand to reach the registered 'point of contact' to resolve security problems. Computing Services shall also have the authority to disconnect any wireless network from the campus network backbone whose traffic patterns seem unusually suspicious or violates practices set forth in this and other policies.

It is the responsibility of the department, centre or unit to be knowledgeable regarding the provision all Computing Services policies.

Grievance and Appeals

Grievances with this policy or conflicts or disputes between Computing Services and any University department, center or unit should be directed to the IT Manager for resolution.

Related Documentation

This policy strongly encourages all users to familiarise themselves with the requirements, conditions and responsibilities of other related internal and external policy and legislative material that will inform their use of the School’s IT services. These related sources are:

- School Regulations
- Computing Service's Acceptable Use Policy
- Computing Guidelines