Addendum to the Staff AUP:

Wireless Access - As AACS begins to deploy wireless network connectivity in its schools, access for non-AACS-owned devices may be approved for use. This approval would come from administration and district technology staff. While connected to the AACS wireless network, the guidelines of this Acceptable Use Policy still apply. AACS reserves the right to search private equipment if there is reasonable suspicion that school policies are being violated, whether or not the equipment is connected to the wireless network. Student and or staff personal devices connecting to the AACS network resources are never allowed. Student and staff personal devices connecting to the AACS public network are never allowed without staff approval and supervision.

Wireless Access Policy

Overview

AACS has wireless networking access available in most locations. As additional equipment is obtained, coverage will be expanded and new protocols (e.g., 802.11g) will be added.

Wireless connections provide access to most of the same services as cabled network ports, although performance may be slower, particularly for certain high-bandwidth services such as streaming video. Wireless networks also introduce certain challenges that are unseen or not as prevalent with cabled networks. These require us to adjust our network practices and access policies in order to ensure high quality secured services.

The primary purpose of this document is to outline and explain changes in network access policies that are required to accommodate campus-wide wireless networking. As wireless services further develop, this interim document will be modified by the appropriate campus technology committee(s) and eventually be integrated into the Acceptable Use Policy for AACS staff.

Special Challenges Introduced by Wireless

A wireless network requires the installation of wireless access points at numerous locations on campus. Each access point has a limited range and bandwidth. As result, performance of the services offered might be limited. Reasonable and reliable performance requires that we minimize interference by controlling the devices that provide or use wireless services.

Unsecured wireless network devices can create significant security issues not only for other nearby wireless devices, but also for devices attached to our cabled network. For example, a single personal laptop computer with both a wireless card and an Ethernet connection can expose a server containing sensitive data to attacks from hackers. Hackers do not need to be directly connected to the cabled network if they can enter through a wireless interface. The owner of the laptop can be entirely unaware that this vulnerability exists and that his/her system is being used as a gateway.

Policy

• All general policies contained within the current Acceptable Use Policy for AACS Facilities apply to wireless network users.

• Computer user devices (e.g., computers, PDAs) connecting to the AACS network by any means can do so only to provide the end user with access to existing information or with the means to communicate new information via email, web, etc. End users are not permitted use of devices to provide unauthorized services or as gateways to provide alternative means of access to AACS services.

• Only the AACS Technology Department (AACS - TD) is authorized to attach wireless hubs or switches (commonly known as Access Points or AP's) to the campus cabled network. Under no circumstances may personally owned AP's or similar devices be connected to open cabled network ports anywhere on campus.

• Computer users' devices, including personal laptop computers with wireless network interfaces, capable of acting as bridges between wireless and wired networks should not be attached to open cabled network ports unless the wireless interface is disabled. Both cabled and wireless networking capability can be simultaneously active even if the end user is unaware of this. This means that users must actively disable their wireless interfaces (e.g., WiFi cards) before attaching to an Ethernet port.

• AACS - TD will monitor the local wireless network for unauthorized AP's and other unauthorized wireless network devices that pose security risks. A first-time violation of any access policy will result in the wired network port associated with an unauthorized device being immediately disabled without warning. An attempt will be made to identify the owner of the unauthorized device and inform him/her of the violation. Subsequent violations may result in more serious measures including the extended loss of access to computing services.

• AACS – TD will be responsible for maintaining a reasonable balance between easy access and proper security for all cabled and wireless network services. In certain cases, some cabled network services may be inaccessible from wireless connections because of security considerations. Individuals wishing to request the addition of a particular service for wireless accessibility or an explanation as to why a particular service is unavailable may contact the AACS helpdesk.

• Wireless network access policies will be updated as technologies rapidly evolve. Every effort will be made to inform the community before a change in network administration practices is dictated by a new technology, but advance notice may not always be possible. Providing reliable and secure access to the most critical services for the overwhelming majority of users will be the single most important consideration in determining policies.

Long Term Wireless users will need to register their wireless network interface device addresses (MAC address) before being allowed to connect to the wireless network

Short Term Wireless users may obtain guest access by requesting the current guest account credentials from the respective location administrator’s office.