WAUBONSEE
COMMUNITY COLLEGE

Wireless Networking Guidelines

Equipment

Integration of wireless network access points or other wireless communications equipment to College network will only be performed by IT. Waubonsee students, faculty, staff, and departments may purchase the Wi-Fi certified wireless network interface adapters of their choice to connect end user devices to the College's wireless networks. College departments will be required to remove any wireless network infrastructure equipment (Wi-Fi routers and bridges) not installed by IT. Wireless network access points will be connected to the College's wired network by means of a specially designated wireless port that will be installed specifically for this purpose. College departments and individuals may not disconnect a wireless access point from its associated wireless port or interfere with any components of the wireless access point assembly including antennas, antenna cables, or management cables. Wireless ports are specially configured to supply electrical power to the wireless access point and may cause permanent damage to an improperly connected end user device. Wireless network installations at College locations consist of the necessary Wi-Fi certified wireless access point devices. The number of access points required will be determined by initial estimates of demand for users and the size of the area to be covered. If the number of users to be served exceeds the practical number of users that can connect to single access point with sufficient bandwidth available to each user, additional access points may be installed. In areas with a high density of users, such as classrooms and lecture halls, additional access points will be installed to satisfy the usage requirements. All wireless access point devices will be installed, and maintained by IT.

Network Reliability

In order to ensure the reliable performance of the College's network, IT will investigate reports of specific wireless devices that are suspected of causing interference and performance problems in the same manner in which IT investigates reports of specific devices connected to wired ports that are suspected of causing disruption. Wireless access service is provided on the basis of anticipated utilization data gathered during initial site surveys conducted by IT. As the number of users increases, effective wireless network performance may be diminished. Current industry standards for wireless network service do not provide sufficient throughput to effectively support bandwidth-intensive applications and network services. IT prohibits the use of serving-based applications (file, web, media-servers) on the College’s wireless network.

Security

Access to the College’s wireless networks will require all authorized users in all areas to authenticate to the network using their assigned College Network/MyWCC Account username and password combinations through the use of college provided wireless client software or 802.1x supplicant. Network

access logs will be maintained containing the username, time of access, and duration of use for all users who access the network using wireless connections and this information can released to the local, state and/or federal authorities if the College is required to release such information.
Wireless technology deployed at the Waubonsee Community College includes the use of WPA 2 (Wi-Fi Protected Access 2), which provides a higher level of security than WPA because AES offers stronger encryption than Temporal Key Integrity Protocol (TKIP). TKIP is the encryption algorithm that WPA uses. WPA 2 creates fresh session keys on every association. The encryption keys that are used for each client on the network are unique and specific to that client. Ultimately, every packet that is sent over the air is encrypted with a unique key. Security is enhanced with the use of a new and unique encryption key because there is no key reuse. The use of WPA 2 and 802.1x for user authentication will provide advanced security levels for the activities of College wireless network users. The College's Central Directory Service will be used as the basis for authentication to services, including wireless network access. Now that Protected Extensible Authentication Protocol (PEAP) and Advanced Encryption Standard (AES) have been deployed, IT will not support older, less secure security methods. Although the security of the wireless network is now comparable with the wired network, the College will prevent wireless access to the sensitive data that is stored on protected servers. Department's using the wireless network in their areas for day-to-day operations will not be granted exceptions through the WCC IT firewalls to gain native access to sensitive information via the wireless network without the use of a VPN (IT Secure VPN Service or IP Sec). College students, faculty, staff and departments must follow the terms of all applicable College acceptable use policies, network usage guidelines and all applicable local, state, and federal regulations when using equipment connected to the College's network whether or not the individual is using wireless or wired network connections. Violations of such guidelines will be reported to the College's computer incident response team and may be forwarded to the appropriate College or governmental authorities. College students, faculty, staff and departments are reminded that the use of wireless network connections may increase the risk that confidential information can be intercepted by unauthorized or unintended parties and that this risk is inherent in wireless network technology irrespective of security measures that can be implemented by the College. Users should avoid sending or receiving confidential or other sensitive data via wireless connections.

Wireless Usage

Some services can have a negative impact on a wireless network because they generate a high level of activity on the network. Such services can negatively affect your wireless network performance and the network performance of other wireless users. The wireless network is a shared resource, which means the bandwidth available to each user of an access point will decline as high-bandwidth services are used. If a student, faculty member or staff member has a need for a service that requires high bandwidth, a wired network connection should be used. The following list provides examples of high bandwidth usage; please note that this list is not all inclusive. You cannot use the computer you have connected to the wireless network as a server of any kind, such as:

- Web servers
- Peer-to-peer file sharing servers
- FTP servers
- Multiplayer game servers

An unsecured computer may have problems that will also result in high bandwidth usage. Following are examples of possible problems:

- Infections by worms or viruses
- Compromised systems running FTP, IRC or other services of malicious spyware programs

Some activities may also use excessive wireless bandwidth. The following are some examples of user activities that consume high amounts of bandwidth:

- Reinstalling an operating system
- Downloading and installing applications
- Performing system backups
- Transferring large files (images, video, music, databases) to other system

Airspace

Problems can occur if other devices use the same radio frequency range (2.4 GHz) as the wireless network. Because of the potential for conflicts it is important for all users to understand which technologies are permitted in our environment and which are not permitted. In order to provide wireless network service at the highest level of quality, all non-client devices that use the 2.4 GHz range should be removed from service in any College building. Only devices that are part of the WCC-Secure wireless network will be permitted to use the 2.4 GHz range. This includes any device that is used as a wireless base station or router, such as the Apple Airport Base Station, or any other wireless router. Microwave ovens, cordless phones, cameras and audio speakers that use the frequency band of 2.4 GHz or 5 GHz should also not be used in areas with wireless coverage. If you think you have an existing system that may use 2.4 GHz radios for transmission, please contact the TAC at 630-466-HELP (4357) to determine if such devices will interfere with wireless network service in your area.

IT Responsibilities

1. Development and maintenance of the wireless standard and wireless guidelines.
2. Installation and maintenance of all equipment supporting wireless network service at the Waubonsee Community College.
3. Investigation and resolution of wireless communication interference problems.
4. Deployment, management and configuration of wireless network access in public areas, classrooms and office areas.
5. Development and implementation of wireless network security protocols and practices.
6. Provision of user training on wireless network security issues and acceptable use of wireless network services.
7. Performance and security monitoring for all installed wireless access points and provision of performance statistics to College departments upon request.
8. Monitoring of the development of wireless network technologies and evaluation of their potential use within the College's wireless infrastructure.
9. Responding to problems reported to the TAC in accordance with standard procedures.

Wireless User Responsibilities

1. Adherence to the wireless network standard and related guidelines established by the Waubonsee Community College.
2. Implementation of recommended security software, hardware settings, patches and protocols on end user equipment used to access the College's wireless networks.
3. Following all relevant College policies and procedures along with federal, state and local laws pertaining to the security of sensitive and confidential data when working with such data on the College’s wireless networks.
4. Installation of wireless network interface adapters according to published instructions.
5. Assumption of responsibility for support and troubleshooting of problems when using wireless network interface adapters not supported by IT.
6. Immediately reporting known misuse or abuse of the wireless network or associated equipment to the TAC.