

ACCEPTABLE USE POLICY FOR WIRELESS NETWORKS ON-CAMPUS

BACKGROUND

The Eastern Mennonite University wireless network is intended to be a convenient supplement to the wired network for general functions, including web browsing, e-mail and printing. Wireless “access points”, located in certain areas of campus; allow suitably equipped and configured computers to make wireless connections to the university network, including the Internet.

Because wireless radio signals are shared by everyone using the same wireless access point, the bandwidth available to each connection decreases and performance deteriorates as the number of users and traffic increases. Distance from the access point, buildings or objects shielding the access point, signal interference, quality of your equipment, battery power and other factors may also impact performance. As such, the wireless network should not be expected to provide the same quality-of-service as the wired network. When reliability and performance are a must, the wired network should be used.

Applications that generate high network traffic do not work well on wireless networks and negatively impact performance for everyone connected to the same access point. In addition, wireless networks are highly sensitive to overlapping frequencies and can present a risk to the integrity and security of the EMU data network. To promote efficient and secure wireless network access, Information Systems (IS) maintains strict standards for the deployment of wireless devices at EMU.

RESTRICTIONS

- A. All wireless access points must be approved by and registered with the IS Help Desk before they are connected to the EMU network.
- B. Broadcast frequencies used by the wireless network may be monitored on EMU property. Devices that generate interference with the EMU wireless network may be subject to restriction or removal.
- C. Use of the wireless network is subject to the general restrictions of the Acceptable Use Policy for Campus Computers & Networks.
- D. Other than “guest” access, only authenticated access to the university's wireless network is permitted. Typically, authentication is provided from software installed by Information Systems at the time a computer is registered for wireless services with the Information Systems Help Desk. Device and connection logs may be used for assessing network problems or identifying unauthorized or unacceptable use of the wireless network.
- E. All data transmitted via wireless connections across the EMU network must be encrypted.
- F. IS will configure wireless devices with client software suitable for authentication and encryption when they are registered with the IS Help Desk. Wireless configuration settings made by IS should not be changed. Doing so could introduce a serious security vulnerability. If the wireless device is not owned by EMU or an EMU employee, a “computer access fee” will be charged for each registered device unless the device is already registered as a wired device.

LIMITED SUPPORT

- A. The wireless network's maximum data speed is significantly lower than the speed of the campus wired network. High bandwidth operations, such as large file transfers, Microsoft Windows system updates, and media sharing with peer-to-peer programs (i.e. KaZaa, Gnutella, or Bearshare) do not constitute acceptable use of the wireless network.
- B. Performance varies and cannot be guaranteed.
- C. Off-campus connections to the wireless network are not permitted.
- D. Devices connecting to the wireless network must be capable of meeting minimum security standards, as defined by Information Systems. Some older devices do not meet these standards, and may not be used on the wireless network.
- E. A very slow “guest” wireless connection is available for persons who visit the campus for brief periods of time. Guests may become authenticated users by registering their wireless devices with the IS Help Desk.

ACCEPTABLE USE POLICY FOR WIRELESS NETWORKS ON-CAMPUS

ON-CAMPUS WIRELESS ACCESS POINTS NOT OWNED BY EMU

The use of non-Information Systems-provided wireless access points, connected to the EMU network, pose a security risk that could give unauthorized or malicious persons access to confidential EMU data. They can also degrade the performance of the Info Systems-provided wireless services on campus.

Because of these risks, Information Systems is restricting the use of wireless access points connected to the EMU network. Only Information Systems-provided access points are allowed outside of dorms and student housing. Specific details are outlined below.

Students: Wireless access points may be used in the dorms, provided that these devices are registered with the Information Systems department and are secured with at least a 128-bit WEP (Wireless Encryption Protocol) key. Student-owned access points may *not* be used outside the dorms. Students wishing to wirelessly connect to the EMU network outside the dorms must use Information Systems-provided (and secured) wireless access points.

Faculty & Staff: Because they often handle confidential EMU data, faculty and staff wishing to use EMU-owned or personally owned wireless devices must use Information Systems-provided (and secured) wireless access points.

All Users: Information Systems-provided access points will become available for EMU users beginning October 1, 2004. For instructions regarding how to use the Information Systems provided secure wireless network see this FAQ on the IS website: <http://www.emu.edu/is/faqs/answer.php?id=93>

IMPORTANT: Many laptops can be configured as access points. Windows allows Internet Connection Sharing across a wireless interface, and Mac OS X and GNU/Linux provide similar features. Enabling these features effectively turns the laptop into an access point. In order to avoid interference with the Information Systems-provided wireless networks these features *must be disabled* while the wireless device is used on the EMU campus.

DEFINITIONS

- A. *Wireless Network (WLAN)* means local area network technology that uses radio frequency spectrum to connect computing devices to university and department wired networks and may connect to the Campus Network Backbone and the Internet. This technology is alternately known as Wi-Fi, Airport or 802.11b/g.
- B. *Access Point (AP)* means electronic hardware that serves as a common connection point for devices in a wireless network. An access point acts as a network hub that is used to connect segments of a network, using transmit and receive antennas instead of ports for access by multiple users of the wireless network. Access points are shared bandwidth devices and can be connected to the wired network, allowing access to the campus network backbone.
- C. *Wireless Device* means a desktop, laptop, handheld, portable, or other computing device with a component installed to provide a wireless network interface.
- D. *Interference* means the degradation of a wireless communication signal caused by electromagnetic radiation or an overlapping frequency generated from another source. Interference can slow down or eliminate a wireless transmission depending on the strength of the interfering signal.
- E. *Client Software* means the software that is installed in a desktop, laptop, handheld, portable, or other computing device to provide an authenticated wireless network connection.
- F. *Guest access* is a very limited and very slow wireless connection that is provided for campus visitors who wish to access the Internet wirelessly. An "Internet only" wireless network service at speeds no greater than typical modem dialup is provided but a WEP key must be obtained from the IS Help Desk or Library in order to use the wireless "guest" connection. All EMU students and employees are urged to register their wireless devices in order to use wireless network services available to authenticated users.