



## **Office of Information Technology**

### **Wireless Access Policy**

The Office of Information Technology's two-fold goal for wireless networking is to provide the best user experience across campus utilizing wireless networking and protect campus network resources. This policy describes how wireless networking fits into Lee College information technology networking services, how wireless services are currently deployed, and how to request wireless networking services. The policy goals are:

- Provide information regarding current and future direction of wireless deployment.
- Develop a framework for a common experience for wireless users across campus.
- Designate a security mechanism for authenticating users to wireless service.
- Develop expectations and guidelines for wireless usage.

This policy governs the installation, operation, and maintenance of all wireless network devices utilizing Lee College Internet Protocol (IP) network space, including private IP space within the college networks and all users of such devices and governs all wireless connections to the campus network backbone, frequency allocation, network assignment, and registration. It also applies to services provided over wireless connections to the campus network backbone for colleges, departments, or divisions of Lee College. OIT will approach the shared use of the wireless radio frequencies in the same way that it manages the shared use of the wired network.

Wireless access points must be operated so as to minimize interference with other wireless access points compliant with this policy and with legitimate unlicensed devices and other unlicensed bands. In the case of interference by otherwise compliant access points and legitimate devices, OIT will work to negotiate acceptable compromise arrangements. If a compromise cannot be reached, the Director of Information Technology will specify a resolution.

OIT will approach the shared use of the wireless radio frequencies in the same way that it manages the shared use of the wired network. All provisions of the Wireless AUP regarding computing, apply equally to both wired and wireless networking. Specific issues pertaining to wireless network devices are outlined below:

- Concealing your identity, or assuming the identity of another (e.g., by sending forged electronic mail).

- Sharing your password or account with the specific exception of staff or faculty members allowing their support personnel to access their accounts in order to provide services appropriate to their job functions.
- Attempting to “crack” or guess other users’ passwords using capturing programs.
- Denying appropriate access to resources to other users (e.g. “ping flooding” another system, sending “mail bombs,” or modifying a login file in order to cause a user to not be able to log in).
- Releasing programs such as viruses, Trojan horses, worms, etc., that disrupt other users, damage software or hardware, disrupt network performance, or replicate themselves for malicious purpose.
- Sending commercial solicitations via electronic mail (i.e. spamming) to individuals or to newsgroups or mailing lists where such advertising is not part of the purpose of the group or list.
- Any “mass mailing” which is solicitous in nature, unless the mailing is in the conduct of Lee College business.
- Reselling of services based on the college network, such as web hosting, mailing services or the selling of shell accounts.
- Running a proxy server which results in inappropriate or unauthorized access to College materials to non-Lee College members.
- Using mail messages to harass or intimidate another person (such as by repeatedly sending unwanted mail or broadcasting unsolicited mail).
- Violations of any local, state or federal laws, such as the distribution of copyright-protected materials (e.g. the distribution of commercial software, music or films in electronic format without appropriate permissions by the owner).
- If reports of disruptions caused by such devices occur, the circumstances will be investigated and could result in removal of the device with the determination to be made by OIT.

By signing below, you are acknowledging that you have read the Lee College Wireless Access Policy and agree to abide by the stated provisions. In consideration for the privilege of using the College wireless system, I hereby release the College, its operators, and any institutions with which they are affiliated from any and all claims and damages of any nature arising from my use of, or inability to use, the system, including, without limitation, the type of damages identified in the College policy and administrative regulations.

I also understand the responsibilities of authorized users and understand that intentional misuse of data and/or computers can result in disciplinary action.

Name: \_\_\_\_\_

Student ID/Empl ID \_\_\_\_\_

Signature \_\_\_\_\_

Verified in SA    Y/N                      Date:                     

Office of Information Technology \_\_\_\_\_

Keep in mind that several categories of devices use radio frequencies in the same range as 802.11b wireless Ethernet and therefore other devices using the same frequencies may disrupt wireless communications. Devices such as cordless phones, microwave ovens, and personal network devices using the Bluetooth technology may interfere. These interferences can be intermittent and very difficult to diagnose. OIT will make every effort to resolve frequency conflicts between wireless access points; however, OIT will not be responsible for resolving problems resulting from non-network wireless devices.

This list should not be considered to be complete or exhaustive. It should, however, serve as a set of examples of obviously inappropriate behaviors. If you are in doubt about the appropriateness of something that you want to do, contact the Office of Information Technology Helpdesk at 281-425-6874 or 832-556-HELP (4357), or send mail to [helpdesk@lee.edu](mailto:helpdesk@lee.edu)

All wireless access points operated on the Lee College campus must comply the college's **Information Resources Acceptable Use Policy**. Exceptions to this policy must be approved by the Director of Information Technology.

### **Enforcement**

A college unit operating a wireless access point that does not appear to be compliant with this policy will be notified by OIT so that the access point may be brought into compliance. Wireless access points not brought into compliance may be denied LEENet access.

Noncompliant wireless network access points not connected to LEENet may be reported to college executive management with recommendations for corrective measures. Operation of a legitimate non-data wireless device in an unlicensed frequency band interfering with college wireless data network access may also be reported to college executive management with recommendations for corrective measures.

In a perceived emergency situation, OIT may take immediate steps to ensure the integrity of the college data network and systems, safeguard the health and safety of college community members and property, or protect the college from liability.

All decisions, notifications, or measures taken under this policy may be appealed to the Office of Information Technology. Appeals should be submitted by e-mail to [iWiFi@lee.edu](mailto:iWiFi@lee.edu).

Send comments to: [iWiFi@lee.edu](mailto:iWiFi@lee.edu)

- All use of wireless access points and devices must comply with applicable laws, regulations, and college policies including FCC regulations and the College's **Information Resources Acceptable Use Policy**.
- College academic and administrative units are responsible and accountable for the operation of any device using unlicensed bands within their physical or administrative areas of responsibility. Only devices compatible with the college's use of these bands may be operated on the college campus.
- Deployment and use of wireless access points must be approved by the college academic or administrative unit responsible for the area where the access points are located.
- College academic and administrative units may implement additional policies to regulate wireless access points or devices located within their physical or administrative areas of responsibility. Such policies should be made available on unit web sites, should refer to this policy, and may not contradict this policy.
- Wireless network access deployment and operation should be consistent with the strategies, directions, and initiatives of the college's **Information Resources Acceptable Use Policy**.

***Departments and users may not install Access Points without permission.***

The use of the airspace may cause problems with the U.Va. wireless network. If you do elect to purchase and set up your own access point, it is likely that it will have to be removed when an access point, which conforms to the U.Va. standard, is installed in your area.

To insure that the integrity of the College network is maintained and that incorrectly configured equipment does not cause interference problems, ITC requires that departments and individuals (including students) who wish to install wireless network access devices anywhere on the College network seek permission to do so by completing the Request Form and sending it to the Wireless Project Manager. Departments and individuals who install such equipment without review by ITC may be required to remove it.

**iWiFi Wireless Access Policy**

**Created: August, 2004**

**Office of Information Technology**

**Director/Chief Information Officer**