Policy on Connection to the College-Wide Wireless LAN

Approved by BOT on 8/11/05

The College-wide Local Area Network (LAN) is managed by the Department of Networking and Telecommunications and maintained as a separate community limited to authorized users on registered equipment. Access is available to eligible College students, faculty, staff and administrators. See the College's Information Technology Policies and Guidelines (www3.sunysuffolk.edu/Administration/IT/Help/policies) for eligibility requirements by group.

The LAN provides browser-based access to the Internet and College Intranet applications. Current locations with wireless capabilities are identified on the Wireless Access Registration page, which is accessed through the College portals. Neither coverage nor bandwidth is guaranteed as connections are subject to RF interference and limited by the number of active users within a coverage area.

The following are the minimal guidelines that govern connections to wireless access points. Added security may be required and implemented based upon the services provided.

1. No individual may connect equipment to an access point without prior authorization and registration.

    a. Individuals wishing to connect equipment via a wireless access point must register their device (laptop or PDA) and abide by the provisions of this document and the College's Information Technology Policies and Guidelines. Access is granted to registered faculty, staff and administrators for the duration of their employment. Registered students are provided access on an annual basis.

    b. Installation of additional software or additional equipment setup may be required on the device to be connected to an access point. Current guidelines are listed on the Wireless Access Registration page.

        i. Any licensing or installation costs must be provided by the device owner or department (for College-owned devices).

        ii. College staff cannot install software or adjust settings on privately owned equipment. While self-service instructions will be provided, installation and setup are the responsibility of the user and the user assumes the responsibility for any damage that may occur during the installation and setup of their equipment.

c. Devices connecting to access points need to be secure. Users of the network are expected to observe safe computing practices, which include the following:

i. Maintaining a current operating system on the registered device, including being up to date on all critical security patches. The College reserves the right to standardize specific access protocols, which may not be supported by the user's operating system. In this case, access points may also have operating system restrictions.

ii. Running virus protection software with a current engine and the latest DAT files.

2. The College reserves the right to remove access for any device found to be compromised by viruses, worms, trojans, malware, spyware, etc. Individuals may request restoration once the device is cleaned and shown to have a current operating system and to be running a current virus protection package.

a. Individuals using devices found to contain applications used for hacking will be subject to disciplinary action, as outlined in the "Violations" section of the College's Information Technology Policies and Guidelines.

3. Individuals make connections to and use the wireless network at their own risk.

a. This network is a secondary service of the Department of Networking and Telecommunications and no claims are made as to its availability, quality of service, or security.

b. While efforts will be made to monitor problems and keep the network free from viruses, worms and unauthorized use, the College does not guarantee any level of security.

c. It is recommended that users only access secure sites (shtml) when transmitting or receiving personal data over the wireless network. Encrypted transmissions are controlled by user software and destination site and are not the responsibility of the College.

4. To insure connectivity and bandwidth for the largest number of users, high-bandwidth applications will be limited or blocked during peak-usage hours. Examples of such applications include the following:

a. Role-playing games

b. Streaming audio and video, and other HTML tunneled protocols

c. Large audio, video, software or data file uploads and downloads

User authorization and equipment registration is available through the College portals. Students should see the Instructions for "Getting Connected" to the SCCC Student Wireless Network (http://depthome.sunysuffolk.edu/Central/Networking/Wireless/HowToReg.pdf) for registration directions. Faculty, staff and administrators should login their portal account and see the information listed under announcements.

Additional help with wireless connections and trouble report procedures can be found in the "College Services" channel of the portals. General information is available through the College homepage under Frequently Asked Questions and indexed as **Wireless Access**.