Roger Williams University – Office of Information Technology

Wireless Airspace Policy

Roger Williams University has implemented wireless networking services on the University campus to promote the convenience of mobile network connectivity. This service allows members of the University community to access the campus-wide network from laptops and personal digital assistants. Accidental or intentional disruption of a wireless network will deprive others of access to important University resources. To provide this service, the radio frequency airspace of the University serves as the transport medium for this technology. Wireless networks operate on the campus shared and finite airspace spectrum.

Current wireless Ethernet is based upon products that use the Federal Communications Commission radio frequency bands of 2.4 GHz and 5GHz. Wireless transmissions within these bands conform to the IEEE 802.11b DSSS (Direct Sequence Spread Spectrum) and IEEE 802.11a, IEEE 802.11b, IEEE 802.11g and IEEE 802.11n wireless LAN specifications. Other wireless products also exist in the marketplace that use these same 2.4 GHz and 5GHz frequency bands but do not conform to these standards. Such products can cause interference to wireless service and can prevent University users from obtaining or maintaining network connectivity. These devices include, but are not limited to, other IEEE wireless LAN devices, bluetooth products, cordless telephones, wireless video cameras, microwave ovens, and wireless audio speakers. Certain wireless LAN products are also more susceptible to unauthorized access due to encryption and security flaws. Therefore, the Office of Information Technology (OIT) will regulate and manage this airspace to ensure its fair and efficient allocation and to prevent collision, interference, unauthorized intrusion and failure. In addition, central management will facilitate the adoption of new features. Persons using wireless devices to connect to the University network must be aware of this, and comply with the policies outlined herein.

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 University policies regarding computing, including the RWU Appropriate Use Policy, apply equally to both wired and wireless networking. Specific issues pertaining to wireless network devices are outlined below:

- Only access points provided and installed by OIT or approved by OIT are permitted on the University network or the campus. A consultation with OIT is available to assist with questions. Should an unauthorized access point be found, the OIT has the option of confiscating the access point or requiring it to be removed. Any person found responsible for the installation of un-authorized access points can be reported to the Office of Human Resources (in the case of employees) or the Office of Judicial Affairs and Community Standards (in the case of a student).

- All access points shall be installed and configured in such a way as to comply with all security features of the wireless network, including restrictions to provide connections only to those users who are entitled to access as members of the University community.
- No access points shall be installed on the Administrative segments of the network. There shall be NO exceptions.
- The University reserves the right to disconnect and remove any access point not installed and configured by OIT personnel or specifically covered by prior written agreement and/or arrangement with OIT. In cases where the device is being used for specific teaching or research applications, OIT will work with faculty to determine how the wireless devices may be used while maintaining required security and without causing interference.
- Other devices such as portable phones, and wireless devices using "Bluetooth" (a competing wireless technology), that broadcast and receive information on the same frequency as wireless Ethernet devices may not be allowed on the network, due to the possibility of interference. 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.

Only users affiliated with Roger Williams University are authorized to use wireless networking on campus. To help protect these affiliated users from unauthorized access to their computer resources, OIT may implement data encryption and authentication security measures that must be followed by all users. These measures require the use of specific wireless LAN product types and are designed to meet emerging wireless encryption and security standards. These measures may include other authentication mechanisms including login etc.