**Wireless Access Policy**

The goal of this policy is to protect Fairfield University’s technology-based resources from unauthorized use that could result in loss of information, damage to critical applications, and/or unauthorized access to secure resources. All users employing wireless methods of accessing university technology resources must adhere to university-defined processes by way of university-provided access points. Unauthorized access to the wireless network is prohibited.

**POLICY**

1. All wireless access points, including wireless routers, that are within the Fairfield University firewall must be approved and centrally managed by the Information Technology Services department (ITS). The addition of new wireless access points within campus facilities will be managed at the sole discretion of ITS. Non-sanctioned installations of wireless equipment, or the use of unauthorized equipment on campus premises, is strictly prohibited.

2. The ITS department will regularly conduct sweeps of the wireless network to ensure there are no unauthorized access points present.

3. The ITS department reserves the right to shut down, without notice, any wired network port to which an unauthorized access point is connected.

4. Any device or equipment found to be interfering with wireless access point signals may be subject to relocation or removal, including cordless phones, microwave ovens, cameras, light ballasts, etc.

Wireless networks are not a replacement for a wired network. As the university’s wireless network is an extension to the existing wired network, wireless access should not be used for work sessions that require the transfer of large amounts of data (e.g., backups or file downloads) or for access to sensitive organizational data.

This policy applies to all campus community members including but not limited to, students, faculty and staff members as well as those holding sponsored, guest, or courtesy accounts.

Wireless access users agree to immediately report to ITS any incident or suspected incidents of unauthorized access point installation. If an unauthorized access point is identified, ITS will request the owner remove the device from the network within 3 business days. If the device is not promptly removed, ITS will disable all network access to the unauthorized access point. If an owner cannot be determined for the unauthorized access point, it will be disabled within 1 business day.

Failure to comply with the Wireless Access Policy may result in the suspension of wireless access privileges and possible disciplinary action.