IT USE GUIDELINE

Wireless Device Connections

Students, Faculty, and Staff bring a variety of devices to our campus. Many of these have options for wireless network connections. In many cases those connections present no problems and are appropriate and welcome. In some cases, however, wireless devices do present problems and can adversely impact other users on the network. This guideline provides information about what can and cannot be properly used on the UA wireless network.

Effective as of: **8/1/2014**

Sponsor and Approvers:

Scott Montgomery - Sponsor

John McGowan, Ashley Ewing, IT Governance - Approvers

Status of Guideline: **Published**

Audience:

This IT Guideline should be observed by:

Students ☒ Faculty ☒ Staff ☒

Contractors/suppliers ☒

Other (specify) ☐ Click here to specify "other".

Statement of need and purpose:

Wireless services are provided on the UA campus by the Office of Information Technology for the use of students, faculty and staff. Not all devices that are capable of wireless network connections work well on general purpose wireless networks. This guideline is needed to clarify what devices can and cannot be supported on the UA wireless network.

Guideline:

The UA wireless network provides WiFi (IEEE 802.11x) network access services. This guideline refers only to this service and does not apply to cellular services. The range of devices that can connect to WiFi services has increased in recent years and continues to do so. Computers, tablet devices, smart phones, gaming devices, Apple TV, and various other devices now have WiFi connection capabilities. But the use of some of these devices (e.g. gaming devices and Apple TVs) create significant issues when used in a

general purpose shared wireless network. Those devices were designed for use on private home networks and work well in those environments. When used in a general shared wireless network environment like the UA WiFi network, they can interfere with the connections of other users and can exceed reasonable bandwidth capacities available, diminishing the available bandwidth for neighboring users.

In most cases, those devices have options for hard-wired connections (i.e. plugging them into a network wall jack). This is the approved and recommended way to connect those devices.

Devices that are generally approved for use on the UA wireless (WiFi) network include laptop computers, tablets (iPad, Android, etc.), and smart phones with WiFi services.

Devices that are not approved for use on the UA wireless (WiFi) network include gaming devices (e.g. Wii, Nintendo, Xbox, etc.), AppleTV, wireless printers, or any other devices not specifically designed for use on a shared general purpose public wireless network.

If there is a need to use non-approved devices, users should consult with OIT on ways to provide the required device access.

Compliance:

Compliance to Guidelines is voluntary but recommended. Not adhering to guidelines can cause disruption to services, security exposures, and/or adverse impacts to other users. Enforcement of guidelines is addressed when deviations cause issues for others or result in known and significant security exposures and are handled through the organizational management structure.