



UNIVERSITY of
SAINT FRANCIS™

Mobile Device Policy

- I. Background**
- II. Purpose**
- III. Policy for Staff and Faculty**
- IV. Policy for students attending USF**
- V. Laptop, Notebooks, and Netbooks**
- VI. Device Support**
- VII. Contacts**

I. Background

The University of Saint Francis has installed wireless access points in all of the buildings at its Fort Wayne, Indiana Campus. Wireless networking is an extension of the University's existing wired network infrastructure and is not intended as a replacement for wired connections. The wireless network allows users with wireless enabled mobile devices to access the University network without having to plug into a network wall outlet. For the purpose of this policy mobile devices are defined as Laptops, Notebooks, Netbooks, PDA's (Personal Digital Assistants), Cell Phones, Smartphones and gaming consoles (wii, Playstation, X box).

II. Purpose

The purpose of this policy is to provide guidance as to what types of mobile devices are allowed on the University's wireless network and to what extent the University will support those devices. The policy will also provide guidance on how to gain access to the wireless network with a mobile device.

For additional information regarding Mobile Computing please see Section 11 of the University's Information Technology Security Policy.

III. Policy for Staff and Faculty

The University allows all staff and faculty with active user accounts to connect to the wireless network using a University owned or personally owned PDA, Cell Phone and/or Smartphone. Due to current Internal Revenue Service Rules concerning "Listed Property", the University will not purchase mobile devices for staff and faculty. The University will continue to honor all contracts for mobile devices purchased prior to July 1, 2009. Those devices will be used for official business only and at no time will be used for personal business.

To connect to the USF wireless network the mobile device must be able to connect to a wireless network using 802.11g, (or earlier) wireless standards. The University does not allow "hacked" devices or devices that have been altered from the manufacturer's original configuration by someone other than the devices original owner to connect to its network. Staff and faculty found connecting to the University's wireless network with these types of devices are subject to discipline in accordance with the University's Information Technology Security Policy.

Once a mobile device has connected to the wireless network the user will be prompted to enter their user name and password. Once a successful logon has occurred the user is free to use the mobile device on the wireless network in accordance with the existing policies of the

University of Saint Francis. It is important to note that it is in violation of the University of Saint Francis' security policy to store confidential and/or sensitive information on a mobile device. Staff and Faculty are responsible for all University data stored on their mobile devices. For this reason it is highly recommended that mobile devices use password protection when not in use in order to prevent unauthorized access to University data.

The University does not allow synching software to be installed on University owned desktops or laptops in order to synch information from those devices to a mobile device. The only exception is for devices requiring synching software that were installed prior to July 1, 2009. After this date no existing software will be installed or re-installed on a University owned machine.

Gaming devices such as Nintendo Wii, Xbox and Playstation owned by Staff and Faculty are not authorized on the University's wireless network.

IV. Policy for Students Attending USF

The University allows Students with active user accounts to connect to the wireless network using a personally owned PDA, Cell Phone, Smartphone and/or gaming device. To connect to the USF wireless network the mobile device must be able to connect to a wireless network using 802.11g, (or earlier) wireless standards. The University does not allow "hacked" devices or devices that have been altered from the manufacturer's original configuration by someone other than the devices original owner to connect to its network. Students found connecting to the University's wireless network with these types of devices are subject to discipline in accordance with the University's Information Technology Security Policy.

Once a mobile device has connected to the wireless network the user will be prompted to enter their user name and password. Once a successful logon has occurred the user is free to use the mobile device on the wireless network in accordance with the existing policies of the University of Saint Francis.

Resident students wishing to connect personally owned gaming devices such as Nintendo Wii, Xbox and Playstation to the wireless network will need to contact the USF Help Desk in order to provide the gaming systems MAC or Ethernet address before it will be authorized to be used on the University's wireless network.

V. Laptops, Notepads, Netbooks

The University allows staff and students with active user accounts to connect to the wireless network using University owned and personally owned Laptops, Notepads, and Netbooks. To connect to the USF wireless network the mobile device must be able to connect to a wireless

network using 802.11g, (or earlier) wireless standards. The University maintains two wireless networks for use by staff, faculty and students.

Staff and Faculty are highly encouraged to log in the encrypted wireless network since this will allow them access to their personal and/or departmental shares and provide a higher degree of security. Logging into the open (un-encrypted) network will not allow access to personal or departmental shares.

When logging into the wireless network with a Laptop, Notepad or Netbook security system will require that your machine be scanned to ensure that it is free of viruses and the virus protection is installed and meets the University minimum standards for virus protection.

For detailed instruction on logging into the wireless network please refer to the User Support Website: <http://www.sf.edu/sf/uts/uss/services/wireless>

VI. Device Support

The extent to which the University of Saint Francis will support a mobile device's connection is limited to authorizing the devices MAC or Ethernet Address onto the wireless network.

Questions or problems concerning the actual mobile device and its settings need to be addressed to the service provider and/or manufacturer of the mobile device

VII. Contacts

Security Questions:

Director of Technology, Security and Compliance, 260-399-7700 x 6019

www.sf.edu/sf/uts/tsc

Reporting an incident:

Director of Technology, Security and Compliance, 260-399-7700 x 6019

www.sf.edu/sf/uts/tsc

Executive Director of University Technology Services, 260-399-7700 x 6020

www.sf.edu/sf/uts