Wireless Network Policy

Approved by NNU Technical Advisory Group (TAG), May 2007
Revision 1.0.....................................September 17, 2012
Wireless Network Policy

Purpose
Northwest Nazarene University’s Information Technology Department maintains a wireless network as a supplement to the campus-wide “wired” network. The wireless network is intended to enhance the educational experience through the use of mobile computing technologies. The wireless network is available to students, faculty and staff via “NNU-Wireless” and is available to campus visitors via “NNU-Visitor”.

NNU-Wireless
NNU-Wireless is available for all students, faculty and staff without additional cost to the user. NNU-Wireless requires an NNU network login username and password in Active Directory. Students, faculty and staff may connect managed wireless computers and their personal devices using their NNU network login credentials.

- Instructions for connecting a personally-owned device to NNU-Wireless can be found, after successful login, on the “Students” or the “Employee” tab at http://my.nnu.edu.
- It is the responsibility of the owner of any device connecting to the NNU-Wireless network to see that their device is patched and updated to safeguard their device and the NNU network from viruses and malware. Failure to do so may result in disconnection of that device from the NNU network.
- NNU-Wireless Internet activity is filtered and all violations of the Computer and Network Use Policy are monitored and logged. Failure to observe the acceptable use policy may result in disconnection from the NNU network.
- The Computer and Network Use Policy is found on the NNU IT web page, www.nnu.edu/it/campus-policies-for-information-technology.
- NNU-Wireless is secured with WPA2-AES Enterprise encryption. It is secure and a safe connection for all forms of Internet activity.
- NNU-Wireless covers the main campus in Nampa and is not a fringe benefit for those who rent the properties owned by the University situated near the campus. No support will be given to users in these rental houses to make sure they have a wireless connection while on those premises.

**NOTE:** The Office of Technology and Media Resources will offer limited assistance to students and employees wishing to connect to NNU-Wireless. However, due to the diversity of devices coming to campus, we offer no guarantees that all devices will be compatible with the NNU-Wireless system.

NNU-Visitor
Official campus visitors and guests are invited to use the NNU-Visitor wireless network as a convenience for conducting personal and business communications on the Nampa campus via the Internet. Campus visitors include: Parents of students, potential students, vendors, special event members, participants and attendees of conferences.
The university makes no guarantee concerning the security, availability, reliability or confidentiality of transmissions made via NNU-Visitor wireless system.

- The NNU-Visitor system is intended for guests and visitors to connect a personally-owned device for Internet access only.
- NNU-Visitor is not intended for use by NNU faculty, staff or students.
- NNU-Visitor is not intended for use by the general public who are in proximity to the campus but have no other authorization to use this network apart from the fact it exists.
- Authorized NNU visitors requesting a key can obtain access to the wireless system by registering with their conference coordinator or by going to the Technology and Media Resources help desk for assistance.
- Visitors will be asked to give a full name (first and last name) to generate a visitor key. (No generic names will be used for visitor keys.)
  - People who are invited to the campus by the following offices may request a wireless access code from the secretary or assistant in that office: Admissions, Conferences & Events, Library, Technology & Media Resources, Alumni, and Dept. of Religion.
- NNU-Visitor Internet activity is filtered and all violations of the acceptable use policy are monitored and logged, and may result in disconnection of the computer from the network.
- It is the responsibility of the owner of any device connecting to the University wireless network to see that their device is patched and updated to safeguard their device and the NNU network from viruses and malware. Failure to do so may result in disconnection of that device from the University wireless network.

**NOTE:** NNU IT personnel will not be responsible for troubleshooting network connection issues on personally-owned devices for campus visitors.