



Please read the following Acceptable Use Policies in their entirety to ensure that you understand all the terms and conditions contained therein:

*Network Acceptable Use Policy*  
*E-Mail Acceptable Use Policy*  
*Internet Acceptable Use Policy*  
*Wireless Acceptable Use Policy*

By using the technology provided by Trevecca Nazarene University, you agree to abide by these policies. **Any violation of these University policies may result in disciplinary action, including the termination of your network, e-mail, and/or internet access.**

## Network Acceptable Use Policy

---

TNU*net* must not be used for any activity that does not support the mission and purposes of Trevecca Nazarene University. If a particular usage is not in the best interest of the University or if it does not support the University's mission and purposes, then it must not be done.

Deliberate disruption of anyone's work or system is expressly prohibited, including any action intended to disrupt normal system services, user accounts or network performance.

Users must not make any unauthorized copies of copyrighted software. Software provided by TNU is purchased under software licensing agreements that place legal restrictions on their use and copying.

TNU*net* must not be used for any unlawful purposes. Specifically, the network must not be used by anyone to transmit threatening, obscene, harassing, or pornographic materials.

Any attempts to penetrate a remote site without proper authorization are strictly forbidden and also violate Tennessee state law.

Users must not intentionally seek information about, browse, copy, or modify files or passwords belonging to other users.

Users must not attempt to decrypt or translate encrypted material not intended for them or obtain system privileges to which they are not entitled. If a network security exposure is encountered or observed, it must be reported to the Office of Information Technology Services (ITS) immediately.

Users must set and maintain a network password that will protect their accounts from unauthorized use. It is a serious violation to use another user's logon name or password for any purpose. Only ITS employees may be authorized under certain circumstances to use another user's network credentials.

Users must avoid wasting network resources. Examples of wasting network resources include excessive game playing (or other trivial applications) and sending chain letters or other frivolous or excessive messages over *TNUnet*.

**The use of p2p (peer-to-peer) "file sharing" applications is strictly prohibited.** First, **Copyright infringement is illegal and subject to federal and civil prosecution.** Second, a large percentage of files being downloaded are indecent, obscene, and a violation of the University's mission and purpose as a Christian institution. Third, the excessive traffic generated by file sharing applications is wasteful of network resources, causing significant problems for all network users.

Users are strictly prohibited from attaching any wired or wireless "network device" to any campus network connection. Such network devices include routers, switches, bridges, access points, or any similar network devices. With the exception of wired hubs (which students may install in their rooms as needed), the installation and configuration of any network devices on the University's network is solely the responsibility of the ITS department.

Users may not run any network services (e.g., DHCP, DNS, WINS, FTP, NAT, etc.) via any kind of file server or web server or host any Internet-based services on a computer or laptop, except in limited situations where such services are required by employees to perform their assigned duties. Requests by an employee to install or host such services must be approved by the unit/department head and submitted to the ITS director for review and approval.

Registration and remediation technology is used by the University to ensure that all devices attached to *TNUnet* are properly registered and meet minimum health standards. This will protect the campus network from unauthorized users and ensure the highest level of network availability and performance for all users.

The University provides wireless service across campus, including all computer labs, classrooms and residential buildings. Consequently, it is a violation of this policy for any student or unauthorized employee to attach or physically connect any kind of wireless device anywhere on the campus network.

If an employee or student installs an unauthorized or unregistered device on the campus network, such device will be confiscated and the offending employee or student will face applicable disciplinary sanctions.

If a user creates or maintains electronically stored data that is important to his or her work or to the University in general, the user is responsible for the backup of that data. Any electronically stored data on *TNUnet* will be copied to tape at regular intervals as preparation for a catastrophic loss of resources; however, users must decide whether or not this method is an adequate substitute for making personal backups of their data. Specifically, it is always the user's responsibility for making personal backups of any data stored on the local drive(s) of his

or her PC, laptop or other desktop device, either to the network account, diskettes, CDs, or tapes.

Users must not create or willfully disseminate computer viruses. Users must install anti-virus software on their PCs, laptops, or other desktop devices and must take adequate steps to ensure that virus signature files are maintained and updated regularly.

Users need to be aware that there are federal, state, and sometimes local laws that govern certain aspects of computer and telecommunications use. Members of the TNU community are expected to respect these laws and to observe and respect University rules and regulations.

Any questionable use must be considered “not acceptable.” In cases where it may be necessary to request an exception to any of these policies, such requests must be submitted in advance to the ITS director for review and possible approval.

Students who do not comply with this policy will be referred to the dean of Student Development for disciplinary action, in conjunction with the *Technology Policy Committee*. Other users who do not comply with this policy will be referred to the Personnel Office for disciplinary action. In all instances, disciplinary action may include, but is not limited to, loss of network account privileges and suspension, withdrawal or termination from the University.

## **E-Mail Acceptable Use Policy**

---

E-mail services are provided by TNUnet and should be used to support the mission and purposes of the University.

E-mail services may be used for incidental personal purposes provided such use:

- Does not directly or indirectly interfere with the operations or e-mail services of the University;
- Does not burden the University with noticeable incremental cost; and
- Does not interfere with the e-mail user’s employment or other obligations to the University.

Users are not permitted to send e-mail solicitations and must not forward e-mail chain letters to any person, on or off campus, except to forward a message to the director of ITS.

Only authorized employees may send broadcast e-mail messages. Unauthorized users are specifically prohibited from using the University’s **Address Book** to harvest e-mail addresses

for bulk e-mail purposes. Requests to send broadcast e-mail messages may be submitted to the ITS **HelpDesk**.

The University offers LISTSERV capabilities. This service is intended for internal use by University employees or students. User requests for “external” LISTSERVs will be approved only when there is a direct benefit to the university that is applicable to our mission, our academic/instructional programs, or our production application systems. LISTSERV requests may be submitted to the ITS **HelpDesk** on the correct form (available from the ITS **HelpDesk**) and requests for external LISTSERVs will be subject to review and approval by the Senior V.P. for Administration and Financial Services.

Users should be aware of the following:

- E-mail is less private than users may anticipate.
- Deleted e-mail may persist on backup facilities and thus be subject to disclosure under state and federal law.
- E-mail stored on University equipment, whether or not created on University equipment, constitutes a University record subject to disclosure.
- The University cannot protect users from receiving e-mail they may find offensive. Faculty, staff, and students are strongly encouraged to use the same personal and professional courtesies and considerations in e-mail as they would in other forms of communication.

## **Internet Acceptable Use Policy**

---

High-speed Internet services are provided by *TNUnet* and should be used to support the mission and purposes of the university.

Web site filtering is performed to block Internet sites that are offensive, malicious, bandwidth intensive, illegal or unethical. Web sites in categories that will be blocked include but are not limited to the following: adult content, gambling, hacking, audio/video streaming, pornography, tastelessness, sexuality and violence.

It is a violation of the **Internet Acceptable Use Policy** for any *TNUnet* user to bypass or attempt to bypass the Web content filtering controls installed on the TNU network.

## Wireless Acceptable Use Policy

---

By the direction of the Cabinet of Trevecca Nazarene University, the ITS department manages the network campus “from the wall-plate to the Internet” to ensure reliability, security, integrity and interoperability. It is also the responsibility of ITS to ensure the integrity, security and appropriate use of the campus “radio space” in terms of wireless networking.

Wireless networking has a multitude of issues that can step on or conflict significantly with our campus services and policies. Specifically, channel allocations, device placement, information exposure and access point configuration all have the potential to disrupt critical campus services or inadvertently distribute private or sensitive information.

Consequently, please be reminded that Trevecca network users are strictly prohibited from attaching any wired or wireless “network device” to any campus network connection. This is solely the responsibility of the ITS department.

### **Authorized Trevecca network users must comply with the following policies:**

1. “Sniffing” or listening in on wired or wireless networks is expressly prohibited except as a troubleshooting procedure by ITS Network Support personnel.
2. Wireless access points and wireless routers that are not managed by ITS are prohibited on Trevecca Nazarene University’s network. If non-standard access points are identified, they will lose connectivity from the network. In addition, wireless gateways (NAT routers) are not allowed.
3. All wireless access for official University business must be WPA or WPA2 encrypted.
4. The **Trevecca-Unplugged** SSID is for University visitors that do not have a Trevecca network username. This SSID is not encrypted and should NOT be used for official University business including student access.
5. **Trevecca-Unplugged** and **Trevecca-Unplugged-Secure** are SSIDs reserved for use only on Access Points owned by Trevecca Nazarene University.

Failure to follow these wireless networking policies and procedures will result in any noncompliant devices losing network connectivity.

If you have any specific questions not addressed above, please contact the **ITS HelpDesk** at (615) 248-1223 for further assistance.