Trevecca Nazarene University
Information Technology
ACCEPTABLE USE POLICIES

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

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.**

Current Acceptable Use Policies for TNU technology include:

- Network Acceptable Use Policy
- E-Mail Acceptable Use Policy
- Internet Acceptable Use Policy
- Wired/Wireless Acceptable Use Policy

Network Acceptable Use Policy

The Trevecca network must not be used for any activity that does not support the mission and purposes of Trevecca Nazarene University.

Deliberate disruption of TNU technology resources is expressly prohibited, including any action intended to disrupt system services, user accounts, network performance, internet access or any other technology resources.

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.

The Trevecca network must not be used for any unlawful purposes. Specifically, resources must not be used by anyone to transmit threatening, obscene, harassing, or pornographic materials.

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

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.

The use of p2p (peer-to-peer) "file sharing" applications is strictly prohibited.

1. **Copyright infringement is illegal and subject to federal and civil prosecution.**
2. A large percentage of files being downloaded are indecent, obscene, and a violation of the University's mission and purpose as a Christian institution.
3. 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 Department for review and approval.

The University provides wireless service across campus, including all computer labs, classrooms and residential buildings.

If anyone other than an authorized employee installs an unauthorized or unregistered device on the campus network, such device will be confiscated, and the offender will face applicable disciplinary sanctions.

Users must not create or willfully disseminate computer viruses. The ITS department will install, configure, and maintain anti-virus software for all TNU owned computers. All others must install anti-virus software on their desktops or laptops and must take adequate steps to ensure that virus signature/update 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 Department for review and possible approval.

Password Protection

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. This includes but is not limited to Trevecca network access or any other TNU related software or online application where individual login credentials are required. Only ITS employees may be authorized under certain circumstances to use another user's credentials. The following criteria must be used for network passwords:

- Password must be at least 12 characters
- Must contain 1 upper case letter, 1 lower case letter, 1 number, and 1 special character
- Password can't be the same as your previous 4 passwords or contain any part of your name
- Password will never expire though users are encouraged to change their passwords anytime they feel their credentials may have been compromised.

E-Mail Acceptable Use Policy

E-mail services are provided by Trevecca 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
- 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 or mass emails. 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.

Users should be aware of the following:

- E-mail is less private than users may anticipate.
- Deleted e-mail may persist in 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 all e-mails they may find offensive
- Employees 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 Trevecca 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 Trevecca network user to bypass or attempt to bypass the Web content filtering controls used on the Trevecca's network.

If a particular website is blocked and a user needs access to this site as part of their employment at TNU or for approved academic purposes, a request to unblock the site must be sent to the ITS Helpdesk. Requests will be considered on a case-by-case basis. The request will be reviewed by the CIO and ultimate approval to unblock a site will come from the EVP for Finance and Administration and/or the University Provost (academic).

Wired/Wireless Acceptable Use Policy

By the direction of the Trevecca Nazarene University Cabinet members, 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 users of TNU's IT resources 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 authorized ITS 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 encrypted.

4. **Trevecca-Wifi, Trevecca-Devices,** and **Trevecca-Guest** are SSIDs reserved for use only on Access Points owned by Trevecca Nazarene University.

5. The **Trevecca-Guest** 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.

6. The **Trevecca-Wifi** and **Trevecca-Devices** SSIDs are encrypted and are required to be used by all TNU employees who utilize wireless connectivity for all TNU owned laptops, smart phones, tablets, or any other TNU owned wireless device that can utilize a secure Wi-Fi connection. These SSIDs are recommended for student use though not required. Students choosing NOT to utilize these secure Wi-Fi connections, do so at their own risk.

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