



Texas Wesleyan University Information & Communication Technology

Policy for the Acceptable Use of Network Resources

Texas Wesleyan University is responsible for securing its network and computing systems in a reasonable and economically feasible degree against unauthorized access and/or abuse, while making them accessible for authorized and legitimate users. This responsibility includes informing users of expected standards of conduct and the punitive measures for not adhering to them. Any attempt to violate the provisions of this policy may result in disciplinary action in the form of temporary revocation of user accounts, regardless of the success or failure of the attempt. Permanent revocations can result from continued abuse.

The users of the network are responsible for respecting and adhering to local, state, federal, and international laws. Any attempt to break those laws through the use of the network may result in litigation against the offender by the proper authorities. If such an event should occur, Texas Wesleyan will fully cooperate with the appropriate authorities to provide any information necessary for the litigation process.

This policy in conjunction with the [Policy for the Acceptable Use of Information Technology Resources](#) will govern the use of information technology resources at Texas Wesleyan University.

University Computing & Telecommunications Operating Policy and Procedures

Network Computing Policy

Once a user receives a user ID to be used to access the network and computer systems on that network, they are solely responsible for all actions taken while using that user ID. Therefore:

1. Applying for a user ID under false pretenses is a punishable disciplinary offense.
2. Sharing your user ID with any other person is prohibited. In the result that you do share your user ID with another person, you will be solely responsible for the actions that other person appropriated.
3. Deletion, examination, copying, or modification of files and/or data belonging to other users without their prior consent is prohibited.
4. Installation of illegal software is prohibited. Unless there is record of clear ownership and legal licensure for the software in question, it should not be installed on any University equipment.
5. Installation of software on a network resource is strictly prohibited. The shared file space on network servers is for the storage of data pertaining to University business only. ICT reserves the right to remove unapproved applications/data from network resources at any time without warning.

6. Attempts to evade or change resource quotas are prohibited. Most users are provided private space on a network resource for storing business-related data. Many users will also have access to other network resources such as access to a departmental/school shared disk space. This space is intended for intra-departmental/school file sharing. This shared space shall not be used for private data storage.
7. Continued impedance of other users through mass consumption of system resources (i.e. misuse of shared disk space, e-mail resources, Internet resources, etc.), after receipt of a request to cease such activity, may result in temporary and/or permanent revocation of the user account.
8. Use of facilities and/or services for commercial purposes is prohibited.
9. Any unauthorized, deliberate action, which damages or disrupts a computing system, alters its normal performance, or causes it to malfunction is a violation regardless of system location or time duration.

Network Security Policy

As a user of the network, you may be allowed to access other networks (and/or the computer systems attached to those networks). Therefore:

- Use of systems and/or networks in attempts to gain unauthorized access to remote systems is prohibited.
- Use of systems and/or networks to connect to other systems, in evasion of the physical limitations of the remote/local system, is prohibited.
- Decryption of system or user passwords is prohibited.
- The copying of system or user passwords is prohibited.
- The copying of copyrighted materials, such as third-party software, without the express written permission of the owner or the proper license, is prohibited.
- Intentional attempts to "crash" network systems or programs are punishable disciplinary offenses.
- Any attempts to secure a higher level of privilege on network systems are punishable disciplinary offenses.
- The willful introduction of computer "viruses" or other disruptive/destructive programs into the campus network or into external networks is prohibited.

Electronic Mail Policy

Whenever you send electronic mail, your name and user ID are included in each mail message. You are responsible for all electronic mail originating from your user ID. Therefore:

- Forgery (or attempted forgery) of electronic mail messages is prohibited.
- Attempts to read, delete, copy, or modify the electronic mail of other users are prohibited.
- Attempts at sending harassing, obscene, and/or other threatening e-mail are prohibited.
- Attempts at sending unsolicited junk mail, "for-profit" messages, or chain letters are prohibited.