TEXAS LUTHERAN UNIVERSITY
POLICY ON USE OF THE TLU COMPUTING ENVIRONMENT

PURPOSE

Texas Lutheran University provides a computing environment within constraints of budget, security and appropriate use considerations that promote the goals and objectives of the university. This policy applies to anyone who uses the university's computers and networks, and it articulates the standards of acceptable use that are expected of all users.

POLICY

The Executive Vice President and Provost is responsible for administering this policy, and for making referrals to appropriate administrative offices for disciplinary action. Any exception to the policy must be approved in writing by the Executive Vice President and Provost.

A. Texas Lutheran University does not guarantee privacy of files stored on campus computers. The university reserves the right to regulate all activity that occurs on the university network or on any other computer-based system owned or leased by the university. Policies include, but are not limited to, the following:

1. Anyone who uses the campus computing environment must have appropriate status (e.g., staff, faculty, emeritus faculty and current students) and must have an established account authorized by the TLU Information Technology Department.

2. Anyone violating university policy should expect any or all of the following disciplinary actions:

    a. Restriction or suspension of access privileges.

    b. Referral to the appropriate disciplinary body of the university.

    c. Referral to the appropriate local, state or federal authority for legal prosecution.

3. Material (software, hardware or data) that is found to be in violation of this policy may be banned and removed from the university computing environment.

4. University system administrators may monitor activity and information on the university network to ensure compliance with this policy.

B. Users must not engage in activity outside the limits of access that have been authorized for them. This includes but is not limited to:

    1. Performing an unauthorized act that impedes the ability of someone else to do his/her work. Examples include but are not limited to:

        a. Tampering with any transmission medium or hardware device, or connecting any unauthorized device or computer to the university network. Examples include but are not limited to:
            a. Routers

b. wireless routers or access points
c. network switches
d. Unregistered gaming devices etc.
e. IP phone systems

b. Intentionally propagating a software virus.

c. Damaging or destroying data owned by the university or someone else.

d. Modifying any disk or software directory provided by the University for any type of special use.

e. Performing an unauthorized act that places an unnecessary load on a shared computer or the university network.

2. Attempting to circumvent protection schemes for access to data or systems, or otherwise uncover security loopholes.

3. Gaining or granting unauthorized access to computers, devices, software or data. This includes, but is not limited to:

a. Admitting someone into a locked facility, or unlocking any facility that is normally locked, without permission.

b. Permitting the use of any account or password, including one's own, in a way that allows unauthorized access to or undue use of computing resources.

4. Use of computing facilities for private gain, profit not associated with university business, or excessive recreational purposes. Examples include but are not limited to:

a. Broadcasting personal messages to large segments of users for advertising or political purposes.

b. Use of university facilities for non-TLU business activities.

c. Pranks or chain messages.

d. Excessive personal use of bandwidth (personal video conferencing, online gaming, etc.)

Incidental personal use of the university's computing resources for occasional e-mail messages, web research, looking up stock quotes, etc. is permissible.

5. Those using computing equipment for purposes other than class work must relinquish the use of the equipment to those performing class-related work, if requested.

C. Users must abide by all applicable laws or government regulations and operate within the limits articulated by the University for ethical and moral behavior. Examples include but are not limited to:

1. Using any material in violation of any software licensing agreement or copyright law.

2. Using software or data that infringes on the rights of others. Examples might include the production or propagation of material that is abusive, profane or sexually, racially or religiously offensive; or material that may injure or harass someone else, or lead to a lawsuit or criminal charges.

3. Using a university equipment or network infrastructure to access off-campus resources (including materials on the Internet) in a manner that is in violation of the ethical or moral standards of the university, as stated in the Student Handbook, Faculty Manual, and Administrative Staff Personnel Handbook.

4. Monitoring someone else's data communications, or otherwise reading, copying, changing or deleting files or software without proper permission of the owner. Students taking courses that require work with computers may be asked to sign a form allowing instructors and/or graders to have access to their files for instructional purposes.

Policy revisions endorsed by the Information Technology Committee on April 29th, 2011, and approved by President's Cabinet – May 2, 2011

Policy revisions endorsed by the Information Technology Committee on November 28th, 2007, and approved by President's Cabinet - February 5, 2008

Policy revisions endorsed by the Information Technology Committee on March 7, 2003 and approved by President's Cabinet - March 24, 2003

Policy revisions endorsed by the Information Technology Committee on April 16, 1999 and approved by President's Council - April 1999

Original policy endorsed by the Information Technology Committee on December 10, 1997 and approved by President's Council - January 1998