

Computer and Network Use Policies

Pacific Lutheran University provides computing and networking resources to students, faculty and staff. Use of these resources is a privilege granted to members of our community as we work and learn in an environment supportive of education and service.

These policies, which apply to all users of PLU's computing and information resources, consist of the following elements:

[General Use Policy](#)
[Network Use Policy](#)
[Anti-Virus Software Policy](#)
[Administrative Systems Use Policy](#)
[Web Policy](#)

Computing and Telecommunications staff members are available to answer questions regarding computer and network use. Feel free to contact them at 535-7525 or comptelc@plu.edu.

Violations and Consequences

The University will take reasonable and necessary steps to preserve the security of its computer and network resources. Doing so maintains a respectful community in which our computing and information resources may be utilized as intended. Users are expected to maintain this community by abiding by computing policies and reporting violations of these policies immediately. Complaints of potential policy violations should be reported to Computing and Telecommunication Services, ext. 7525 or e-mail to comptelc@plu.edu.

Violations of the Policy alleged to have been committed may be referred to the Student Conduct Coordinator, the Director of Human Resources, the Provost, or another appropriate University Officer.

Activities that in any way conflict with these policies can result in sanctions, corresponding to the severity of the action and ranging from a written reprimand to expulsion (for students) and/or referral to the appropriate legal authorities.

The University reserves the right to access electronic communication or data (e.g., email, computer files) as it deems necessary. While the University rarely does this, at times it may be compelled to do so in the enforcement of University policies and ethics, or by an external law enforcement agency.

General Use Policy [\(top\)](#)

Pacific Lutheran University students, faculty, and staff are responsible for legal and ethical use of computers and the network.

Activities considered to be in conflict with this policy include, but are not limited to, the following:

- Spreading viruses or causing disruptions on the network.
- Unauthorized access to restricted or personal computers, data, or programs or knowing use of restricted computers, data or programs accessed or acquired by someone else.
- Sharing a password or account(s). Account holders are responsible and will be held accountable for all activity occurring on their accounts.
- Creating, modifying, executing or re-transmitting any computer program or instructions intended to gain unauthorized access to, or make unauthorized use of, any computer facilities or software.
- Violating copyright laws or software license agreements.
- Installing software, including freeware, shareware, public-domain or commercial software on any university-owned computer equipment without appropriate authority.
- Using computers or networks with the intent to compromise any other computers or networks or to commit crimes or other unethical acts.
- Using computers or networks for unauthorized non-University-related commercial or for-profit activity.
- Sending or forwarding electronic mail for unauthorized purposes (i.e., spam). This includes but is not limited to unsolicited and unsanctioned mass mailings. University officials authorized to send or approve mass electronic mailings are the President, Provost and V.P. for Admission and Student Life
- Viewing, printing, storage, display, or playing of sounds of any sexually explicit or potentially offensive materials in a way that may create an offensive working or learning environment.
- Excessive use of paper, toner, disk space, or other resources.
- Monopolizing systems so that others are prevented from use.
- Overloading computers or networks with excessive data.
- Activities in violation of faculty and staff employment handbooks or student conduct policies (the PLU Code of Conduct).
- Using email or other electronic methods for purposes of harassment or stalking.
- Activities which violate local, state, or federal laws.
- Removing any PLU owned computer software or hardware from campus without written permission of the appropriate administrator.

Network Use Policy [\(top\)](#)

This policy applies to all persons connecting personally-owned computer systems to the Pacific Lutheran University network.

The PLU network includes shared, finite resources installed by the University to promote scholarship and learning for all students. Disruption of the network will deprive others of access to important University resources.

Responsibilities for Personally Owned Computers

To comply with the PLU General Use Policy (<http://www.plu.edu/~comptelc/policies>) and PLU Network Use Policy, users must:

- Maintain a valid, regularly updated anti-virus program. (See the anti-virus web page at: <http://www.plu.edu/antivirus>);
- Maintain effective security practices on the personally owned computer system to avoid intentional or unintentional activities from or to any network connection. Included, but not limited to, are attempts to monitor other network connections, hijack connections, spread viruses, spyware, or any other activity which may impact the overall security of the network; and
- Obtain authorization prior to operating a server on the PLU network. Contact Computing and Telecommunication Services for technical guidance and restrictions.

PLU's Responsibility for the Network

In service to the greater good of the community, the University commits to:

- Ensure wherever possible reliable and continuous connections to the PLU network. (System notices for unexpected network events are found at <http://www.plu.edu/status>)
- Provide timely responses to requests for assistance in the event of a connection failure
- Terminate connections at any time if there is a reasonable and necessary requirement to do so to maintain network service to the University.

Anti-Virus Software Policy [\(top\)](#)

This policy is in effect beginning September 2006.

Anyone who connects a personally owned computer to the PLU network is required to install and regularly update a reliable anti-virus program. The owner is also responsible for the security of the personally owned computer. Failure to assume responsibility for either security or anti-virus protection can result in network interruptions since an unprotected computer is vulnerable to intrusion by anyone in the world. Such intrusion is typically without the owner's knowledge.

- PLU provides students and employees with anti-virus software free of charge for personal computers used on campus.
- This software subscription must be renewed each year. Instructions to download and install the software are made available on the University's web site and otherwise conveyed to all members of the PLU community prior to the beginning of each school year.
- If the individual already has purchased a reliable anti-virus software program, it must continue to be updated regularly.

Specific Consequences for Non-compliance with This Policy

1st Incident

- If a computer is found to contain a virus, the computer will be temporarily removed from the network and the owner will be notified via email and/or telephone.
- The computer will need to be "cleaned" prior to accessing the PLU network. If the user is able to clean the computer, the user will then need to provide evidence of the cleaning prior to reconnection to the network.
- Students may enlist the Help Desk staff to clean the computer.
- Faculty and staff should consult the Help Desk staff for direction.

2nd Incident

- If a second incident of a virus infection occurs, the computer will be temporarily removed from the network and the owner will be notified via email and/or telephone.
- The owner will be charged \$50 before the computer can be reconnected to the network. If the PLU Help Desk determines that the infected machine had been infected even though appropriate steps were taken to protect it, e.g., latest virus definitions were on the computer, a charge would not apply.
- The computer will need to be "cleaned" prior to accessing the PLU network. If the user is able to clean the computer, the user will then need to provide evidence of the cleaning prior to reconnection to the network.
- Students may enlist the Help Desk staff to clean the computer.
- For students, other sanctions may include but are not limited to referral to Student Conduct

3rd Incident

- The stipulations are similar to those in the 2nd incident except that the owner will be charged \$75 to be reconnected to the network.

4th Incident

- In the event of a fourth incident, the computer will be disconnected from the network (put in 'lock-down') and the owner notified by email and/or telephone.
- Student violations will be referred to Student Conduct for additional sanctions, including but not limited to an extended period of loss of the network connection. The length of time will be determined in collaboration with the Dean for Information & Technology Services based on the impact to network services.

Administrative Systems Use Policy [\(top\)](#)

Pacific Lutheran University's administrative computing systems collect and store sensitive data on employees and students that is needed for the normal operations of the University. PLU employees, including student workers, must assume responsibility for legal and ethical computer, data, and network use. This data may include but is not limited to:

- Personal (non-public) information on students, employees, or university affiliates
- University financial information
- Other proprietary University information

Activities considered to be in conflict with this policy include, but are not limited to, the following:

- Unauthorized change, deletion, corruption, or removal of University data from University systems.
- Sharing or using this information for any purpose other than University business.
- Sharing directories and/or files on your computer with others without appropriate authorization or security measures.
- Distributing information that violates the University FERPA Policy. (The University FERPA policy is managed by the Office of Student Life.)
- Transport of restricted or sensitive data via portable media (e.g., flash memory, laptop computer, personal digital assistant) without prior authorization from a PLU vice president in coordination with the Dean for Information & Technology Services.

Web Policy [\(top\)](#)

The PLU web site contains information for and about the PLU community and is a major means of communication, publication and collaboration in support of the mission of the University. The University maintains the right to temporarily disable access to any Web page under review for possible policy violations as well as web pages containing inaccurate information reflecting upon the integrity of the University.

- Any member of the PLU community posting information on the web must abide by U.S. and international copyright and licensing laws. Copyrighted material reproduced on the web site must have prior written permission of the copyright holder.
- All published information will include identification of the owner, date modified or created, and contact information.
- Commercial use of PLU web pages is prohibited.
- Owner(s) of published information are responsible for the accuracy and maintenance of content.

PLU is not responsible for the content of individual home pages, links from these pages, or material accessed via those links.