

Payne Theological Seminary

Information Services Technology Usage Policy

Version 1.0

Payne Theological Seminary (the “Seminary”) encourages the use and application of information technologies by students, faculty, and staff to support the mission of this institution. Computers and computer networks are powerful enabling technologies for accessing and distributing the information and knowledge developed at the Seminary and elsewhere. As such, they are strategic technologies for the current and future needs of the Seminary. The rights of academic freedom and freedom of expression apply to the use of Seminary computer resources. So too, however, do the responsibilities and limitations associated with those rights. The Seminary supports a campus computing environment open to the free expression of ideas, including unpopular points of view. However, the use of resources and activities is subject to the requirements of legal and ethical behavior and Seminary rules and policies. Thus, legitimate use of a computer, computer system or computer network does not extend to whatever is technically possible. Rather, users of Seminary information resources must respect software copyrights and licenses, respect the integrity of access, and respect the rights of other computer users. Users are solely responsible for ascertaining what authorizations are necessary and for obtaining the appropriate authorizations before using Seminary computing resources. This policy covers appropriate use of computers, computer networks, and information contained therein.

As a condition of using the Seminary’s computers, every user acknowledges that he or she has read, understands and agrees to be bound by the terms hereof.

GENERAL PROVISIONS

1. Users of Seminary computing resources must comply with federal and state statutes and laws, Seminary rules and policies, and the terms of applicable contracts including software licenses. Examples of applicable laws, rules, and policies include the laws of libel, privacy, copyright, trademark, obscenity, child pornography, the Electronic Communications Privacy Act, the Computer Fraud and Abuse Act (which prohibit “hacking”, “cracking”, and similar activities), the Seminary’s Student Code of Conduct, and the Seminary’s Harassment Policy.

Computer software is a form of intellectual property controlled by licenses that spell out clearly how it may be used and distributed. All members of the Seminary community (faculty, staff, students, and community patrons), must

adhere to all license provisions regulating the use and distribution of computer software. Use or distribution of software in violation of license provisions may subject the violator to criminal and civil penalties, as well as to civil liability to the licensor. Any violation of licensing agreements, such as copying, distributing, or otherwise sharing of software in violation of the license agreement is prohibited.

A computer network provides a powerful tool in the educational arena by enabling communications and learning among people who are engaged in the education process, but are separated by time, distance, language, or other traditional communication barriers. The unlawful or inappropriate use of these tools infringes on both the integrity of the system and on the rights of others. In that light, the Seminary expects all members of its community to use electronic communications in a responsible, considerate, ethical, and beneficial manner. All users are expected to:

- Respect the rights of all users on the system
 - Comply with all copyright and fair use laws and regulations
 - Comply with any and all applicable instructions issued by faculty and network administrator(s)
 - Use computer network resources (including time on-line and storage) only for purposes directly related to their role at the Seminary
 - Refrain from transmitting defamatory utterances concerning a person, organization, or institution that may subject the individual or Seminary to civil liability damages
2. Anything that is not in keeping with the interests that support the mission of the Seminary and increases the expense of information technology resources is prohibited. This includes the prohibition of the use of Seminary property for private gain.

Any activity that an individual knows or should know is wasteful of computing resources is prohibited. This may include activities such as:

- Sending advertisements for commercial enterprises
- Sending mass mailings or chain letters
- Obtaining unnecessary output
- Maintaining unnecessary or excessive file storage

- Creating unnecessary multiple jobs or processes
- Creating unnecessary network traffic

As with all Seminary resources, the Seminary bears the responsibility and has the authority to allocate, limit or prohibit access to computer and network resources in order to ensure their most effective and economical use.

3. Any action that may destroy, endanger, or divert another's research or writing is prohibited. In addition, Seminary policy prohibits users from gaining access to, using, reviewing, changing, transmitting or deleting another user's files or software without the express permission of the user. Introduction of destructive software such as programs known as computer viruses, Trojan horse or worms into any computer, program, system or network is prohibited. "User" does not apply to the Seminary personnel managing or administering the technology of the institution or the system.

Among the most valuable and most sensitive of the Seminary's computer resources are the personal work and storage spaces assigned to users. The Seminary treats electronically stored information, including personal files, as confidential and permits examination or disclosure of their contents only when authorized by the owner of the information or when required by local, state, or federal law. It is a crime to attempt or to achieve access to, communication, examination, or modification of, to destroy, disclose, use, or take data, computer programs or supporting documentation. In plain words, state law prohibits both the use, transmittal, change, or deletion of another user's files or software without permission and the introduction of destructive software, such as programs known as computer viruses, Trojan horses or worms into any computer, computer system, or network.

4. Anything that may hinder a free and open atmosphere of electronic discussion is prohibited.

Cruelty, obscenity, crudity, and offensiveness, for the sake of offensiveness, have no place in the public discourse of a Seminary community. As members of the Seminary community, we are all responsible to one another and to the thinking and thoughtful community of which each of us ought to be a valuable part. Each of us must be considerate of other users of Seminary computer resources and facilities.

For your information, use of campus e-mail, the Internet, or networks for the following purposes have been subject to criminal, civil, and/or Seminary sanctions at other institutions:

- Threats against persons or property;

- False information about academic or administrative policies or issues;
- Messages deemed offensive to the receiver because of their pointlessly hateful, obscene, harassing, or libelous content.

The foregoing does not include all the kinds of conduct that have been challenged as illegal or inappropriate in a Seminary setting. A good rule of thumb is to refrain from saying anything on any network or computer system that you would not say face to face to another person. Hurtful or offensive words spoken face to face or by telephone leave no written evidence to use against you, but hurtful or offensive words typed on a network or computer system can leave a permanent record that can, depending upon their content, support criminal or civil liability, damage your professional reputation or diminish your stature in the eyes of those whose respect you would like to keep or earn. You should be aware that e-mail files have been ruled to be “discoverable” in a court of law, which means that your privilege of confidentiality is certainly not absolute, but may be overridden by court order.

5. Anything that makes the Seminary or an individual criminally or civilly liable is strictly prohibited.

Any act or omission that may subject an individual or the Seminary to criminal penalties or civil liability is prohibited. The individual responsible for the act or omission may be required to reimburse the Seminary for the full amount of the expense incurred. Each individual must be aware of any state or federal law that imposes civil or criminal liability. If state or federal law prescribes certain consequences for certain conduct, you and the Seminary may suffer those consequences, even if not described herein.

6. The Seminary may employ various measures to protect the security of its computing resources and the privacy of its users.

Access to the computers and to the information technology networked environment within the Seminary is a privilege extended in good faith to students, faculty, staff, and community patrons. To protect the system and the right of all users, inappropriate use of the system will not be tolerated. In addition, while the Seminary does not condone the routine inspection of electronic files, it does reserve the absolute right to place restrictions on the use of its computers and network systems and to establish policies and procedures to ensure that systems operate effectively and legally.

Users should be aware, therefore, that the Seminary cannot guarantee security and confidentiality. Users should therefore engage in “safe computing”. It is the responsibility of each user to protect his/her user identifier (ID) and password from unauthorized use by other individuals. Each user is responsible for the activities that originate from his/her system while

logged onto the network. Users may not lend their network/Internet account and/or password to other users. Any user who has reason to believe that his/her password or ID has been or could have been obtained by another individual must report this to an administrator of the Seminary immediately.

All members of the Seminary community are responsible for ensuring that their handling of information about individuals is consistent with the Seminary's policy on privacy of information. The privacy of individuals must be protected, regardless of the form or location in which the information is stored, including computer media. Access to personal information must be limited to authorized users for approved purposes. Such information must be safeguarded from unauthorized access. Individuals who are authorized to access personal information about others should not make unauthorized disclosure or use of it.

7. Computers and other campus technology are and at all times shall remain Seminary property. The Seminary reserves the right at any time, in its sole discretion, to access, examine, modify, disclose, remove or delete any data, program or document from its computers, system, network or any software program. Such action must be authorized by the Seminary President.

Violations

Penalties may include, but are not limited to, suspension or revocation of user privileges. Such penalties may be assessed for students by their instructors and for all users by the network administrator(s). Decisions may be appealed to the Director of Student and Community Services. Violators may also be billed for illegal use of the computer systems and for any damages caused by such misuse. Violations of this Technology Usage Policy may also constitute violations of other Seminary policies as printed in the handbooks for students, faculty, staff, and adjunct faculty and, as such, violators will be subject to processes and penalties associated with these other Seminary policies as well as applicable local, state and federal laws.

Agreement

By using Seminary computer systems or networks, students, faculty, staff and guests agree to indemnify and hold harmless the Seminary, its employees and agents, from and against any claim, demand, liability, cause of action, or suit for damages arising out of use of Seminary computers, including, but not limited to, any loss of the individual's data stored on the network.

Users must acknowledge their understanding of this general policy as a condition of receiving an account and using the Seminary network to access the Internet. Users will receive a copy of this policy and, upon request, have the opportunity

for explanation and discussion thereof prior to receiving their password. Policies will also be posted in Seminary computer labs and may be accessed on-line.

All Seminary computer system and network users will be deemed to have agreed to this Technology Usage Policy upon entry into the system by use of their password and ID on each occasion of said use. The Seminary hereby expressly and explicitly disclaims any liability and/or responsibility for violations of this policy.

End User Name	Signature	Date
---------------	-----------	------