SEWANEE
THE UNIVERSITY OF THE SOUTH

Policy on Appropriate Use of Information Technology

The following policy applies to the entire University community. The policy addresses the responsible use of information and technology resources, violation of policy, and guidelines for effective use of the University's technology resources, including, but not limited to, hardware, data, and the network. Individuals are also subject to federal, state and local laws governing interactions that occur on the Internet. The University reserves the right to terminate service to any user who does not use our information technology resources responsibly. This policy and guidelines are subject to change at the discretion of the University.

Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to works of all authors and publishers in all media. It encompasses respect for the right to acknowledgment, the right of privacy, and the right to determine the form, manner, and terms of Publication and distribution. Because electronic information is volatile and easily reproduced respect for the work and personal expression of others is especially critical in computer environments. Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorized access, and trade secret and copyright violations, may be grounds for sanctions against members of the academic community.

The Sewanee Responsible Use Policy is to serve as a guideline by which faculty, staff and students can review the requirements of ethical and legal behavior within the University community when using a computer, computer system, network or the Internet. Everyone within the University community who uses University computing and network facilities has the responsibility to use them in an ethical, professional, and legal manner.

Access to and use of computing and networking resources at Sewanee are privileges extended to members of the Sewanee community. The use of University computing resources, like any other University-related activity, is subject to the normal requirements of legal and ethical behavior within the University community. Members of the University community may use these resources for purposes related to their studies, their responsibilities for providing instruction, their duties as employees, their official business with the University, and other University-sanctioned or authorized activities.

The University acknowledges that occasionally faculty, staff and students use University resources assigned to them or to which they are granted access for noncommercial, personal use. Such occasional noncommercial uses are permitted by faculty, staff and students, if they are not excessive, do not interfere with the performance of any faculty, staff, and students, do not interfere with the efficient operation of the University or its

computing resources, and not otherwise prohibited by this policy or any other University policy or directive.

Because computing systems have such great power, activities that might at first seem to be merely mischievous can harm an entire University community and beyond. Any unauthorized access or interference with system functionality is unacceptable. University wide guidelines such as the Student Handbook, Discrimination, Harassment, Sexual Misconduct and Retaliation Policy and Copyright Policy apply to the use of computing resources as do community standards of consideration for others, and the mission of University, Federal, state and local laws and regulations also apply.

The University's computing resources may only be used for legal purposes and may not be used for any of the following purposes or any other purposes that is illegal, immoral, unethical, dishonest, damaging to the reputation of the University, inconsistent with the mission of the University or likely to subject the University to liability. Impermissible uses (some of which may constitute illegal uses), but are not limited to the following:

- Harassment
- Libel or slander
- Fraud or misrepresentation
- Destruction of or damage to equipment, software, or data belonging to the University or others
- Disruption or unauthorized monitoring of electronic communications
- Unauthorized copy or transmission of copy-right protected material
- Use of the Univesity's trademarks, logo, insignia, or copyrights without prior approval
- Violation of computer system security
- Unauthorized use of computer accounts, access codes (Including passwords) or network identification numbers (including e-mail addresses) assigned to others
- Use of computer communications facilities in ways that unnecessarily impede the computing activities of others
- Use of computer communications facilities in ways that unnecessarily impede the computing progress of others
- Develop or use of unapproved mailing list
- Use of computer facilities for private business purposes unrelated to the mission of the University or to University life
- Academic dishonesty
- Violation of software license agreements
- Violation of network usage policies and regulations
- Violation of privacy
- Viewing, posting or sending obscene, pornographic, sexually explicit, or offensive material
- Posting or sending material that is contrary to the mission and values of the University
- Intentional or negligent distribution of computer viruses

Responsibilities of Users

The user is responsible for correct and sufficient use of the tools available for maintaining the security of information stored on each computer system. The following precautions are strongly recommended:

- Computer accounts, passwords, and other types for authorization are not be shared with others
- Understand the level or protection the computer systems automatically apply to files
- Be aware of computer viruses and other destructive computer programs, and take steps to avoid them of the use's privacy or loss of data
- Respect the privacy of others
- Be sure to comply with all federal, state an other applicable laws as well as College policies and regulations

Security

The University will assume that users are aware that electronic files are not necessarily secure. Users of electronic mail systems should be aware that electronic mail is generally not secured and is extremely vulnerable to unauthorized access and modification. The Office of LITS will make available to interested persons information concerning reasonable methods for attempting to protect information on central computing systems from loss, tampering, unauthorized search, or other access.

Privacy and Confidentiality

The University reserves the right to inspect and examine any University owned or operated communications system, computing resource, and/or files or information contained therein at any time, as well as personally owned computers linked to University servers or data network.

Authorized access to data or information entails both privilege and responsibility, not only for the user, but also for the system administrator. There is no expectation of privacy or confidentiality for documents and messages stored on University-owned equipment. Additionally, email and data stored on the University's network of computers may be accessed by the University for the following purposes:

- Troubleshooting hardware or software problems
- Preventing unauthorized access and system misuse
- Retrieving business related information*
- Investigating reports of violation of University policy or local, state or federal law*
- Complying with legal requests for information*
- Rerouting or disposing of undeliverable mail

*The system administrator will need specific approval from the Office of General Counsel or the appropriate designee to access these items. The extent of the access will be limited to what is essentially necessary to acquire the information.

Reporting violations

All users should report any discovered unauthorized access attempts or other improper usage of University owned computers, networks, or other information processing equipment. If you observe, or have reported to you, a security or abuse problem, with any University computer or network facilities, including violation of this policy, you should notify the Chief Technology Officer, the Office of Human Resources or other appropriate administrator.

Violations of this policy may be treated as violation of University policy and/or violations of civil or criminal law. The Office of LITS in conjunction with the Office of Human Resources will investigate apparent or alleged violations of these guidelines. The University reserves the right to immediately suspend user privileges pending investigation. Such action will be taken to protect the security and integrity of the computer system and will take precedence over its impact on the individual's work.

When appropriate, at the discretion of the Chief Technology Officer, cases of apparent abuse will be reported to the Deans of Students (student cases). The Deans of the College and School of Theology (faculty cases), or the Director of Human Resources (staff cases). These offices are responsible for determining any further disciplinary action. Upon a finding of a violation, disciplinary measures may include warnings, suspension of user privileges (temporary or permanent), disciplinary action up to and including termination of employment. The college may also pursue civil and/or criminal charges if it deems appropriate.