SOUTHERN NAZARENE UNIVERSITY
Computer Use & Ethics Policy

Underlying Principles

This Computer Use & Ethics Policy relates to use of all computer facilities operated by the University by students, employees, or guests for any purpose. The University makes available computer facilities primarily for the use of students, faculty, and staff for purposes of research and instruction. We aspire that such facilities be used in faithful accord with the ethical perspective of the Church of the Nazarene and the Wesleyan-Arminian theological tradition.

Respect for intellectual labor and creativity is vital to academic discourse and to the learning enterprise. This principle applies to works of all authors and publishers in all media. It encompasses respect for the right to acknowledgment, right to privacy, and right to determine the form, manner and terms of publication and distribution.

Because electronic information is so 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 and copyright violations, may be grounds for sanctions against members of the academic community.

The following principles and guidelines related to academic honesty, copyright, privacy, security, and appropriate use have been established to facilitate the ethical and responsible use of computers. Instructors or departments may impose additional requirements or restrictions in connection with course or departmental work.

Guidelines

Academic Honesty & Intellectual Theft

Originality, derivation, and the acknowledgement of sources and collaboration are essential to scholarship and the progress of knowledge. Respect for the work and personal expression of others is especially critical in computer environments. Plagiarism and copyright violations infringe on authorial integrity and are grounds for sanctions.

Students are expected to avoid all forms of academic dishonesty, including plagiarism, misrepresentation of authorship, and inappropriate collaboration on assignments. The Office of Academic Affairs will be notified of occurrences of academic dishonesty.

Examples of academic dishonesty include such cases as the following:

- Turning in or submitting electronically someone else's work as your own (with or without his or her knowledge)
- Allowing someone else to turn in or submit electronically your work as his or her own
- Several people's completing an assignment and turning in or submitting electronically multiple copies, all represented either implicitly or explicitly as individual work
- Using any part of someone else's work without proper acknowledgement
- Stealing a solution from an instructor
- Submitting work products that are substantially similar on an assignment that calls for independent work (for example, academic dishonesty in a computer assignment will be suspected if an assignment that calls for independent work results in two or more solutions so similar that one can be converted to another by a mechanical transformation)

Examples of academically honest practices include cases such as the following:

- Turning in or submitting electronically work done alone or with the help of the course's staff

- Submitting one assignment for a group of students if group work is explicitly permitted or required
- Getting or giving help on how to solve minor syntax errors
- Discussing assignments to clarify what to do and how to do it

Copyright

The interests of authors, inventors and software developers in their products are protected by United States copyright and patent laws. Software license agreements serve to increase compliance with copyright and patent laws, and to help insure publishers, authors, and developers return on their investments.

Violating the copyrights or patents of computer software is against University policy and is a violation of state or federal law. Making your own copies of software having a restricted use license is theft.

It is against University policy to violate software agreements. The number of software users must not exceed the purchased software licensing.

The Digital Millennium Copyright Act of 1998 prohibits copying and/or distributing digital media files on the network. The network automatically blocks attempts to download or share files illegally.

Privacy

Students, faculty, and staff who use the computer have the right to privacy and security of their computer programs and data. At the same time, University ownership of the computer system network implies a limited expectation of privacy. The University reserves the right to view and/or retrieve any file or software stored on the computer or passing through the network.

Computer users should not tamper with files or information that belongs to other users or to the operating system.

Reading someone else's electronic mail is a federal offense (Title 18 of the United States Code Section 2701). Computer system administrators are excluded for technical reasons. They are, however, prohibited from disclosing a user's e-mail traffic to anyone, unless the user or the other party to the traffic gives permission.

Security

Owners and users of computer networks operate in an interdependent environment that necessitates joint ownership of institutional information. Reliability and accessibility of information is critical to the successful operations of the University.

Accessing a computer system without authorization is a federal offense (Title 18 of the United States Code Section 2701).

Computer users must not attempt to modify system facilities or attempt to crash the system. Users should not attempt to subvert the restrictions associated with their computer accounts, the networks of which the University is a member, or microcomputer software protections.

Loopholes in computer security systems or knowledge of a special password should not be used to breach security by

- damaging computer systems or degrade the performance of a computer system
- obtaining extra resources or taking resources from another user
- gaining access to systems or use systems for which proper authorization has not been given

- falsifying University records, forms or other documents
- tampering with or destroying the work of others

Appropriate Use

The primary purpose of computer communications systems and networks in an academic environment is to promote the free exchange of ideas and information, thus enhancing teaching and research. All on-line communications and behavior should respect the Wesleyan theological perspective of Southern Nazarene University.

The University prohibits the use of computing resources to intimidate or create an atmosphere of harassment based upon gender, race, religion, ethnic origin, creed, or sexual orientation.

Fraudulent, threatening, or obscene e-mail or graphical displays or audio files used to harass or intimidate are prohibited.

Chain letters, mass mailings, and campus-wide network broadcast messages are also examples of inappropriate uses of University electronic communications resources.

The use of University computers for commercial purposes requires prior approval by the Vice President of Academic Affairs.

Enforcement

The University reserves the right to examine computer files as necessary to enforce these policies. Use of this computing system in any way contrary to applicable Federal or State statutes or the policies of Southern Nazarene University is prohibited and will make users subject to University disciplinary actions and may also subject users to criminal penalties.

Violations of these policies and guidelines may result in the loss of a user's computer use privileges. These privileges may be suspended immediately upon the discovery of a violation of these guidelines. The account may be removed or deactivated or privileges removed from one or all University computing systems permanently or until the matter is completely resolved.

SNU personnel discovering violations of these policies should report to their direct supervisor, who will report incidents to the appropriate office (Academic Affairs, Student Development, or Human Resources). Information related to violations will be shared among these offices and the appropriate disciplinary procedures will be followed in keeping with University policy for students and employees.

Violations of these policies will be dealt with in the same manner as violations of other University policies and may result in disciplinary review. In such a review, the full range of disciplinary sanctions is available. These include, but are not limited to, the loss of computer use privileges, immediate dismissal from the University, and legal action. Violations of some of the above policies may constitute a criminal offense. Criminal offenses may be subject to a fine of not more than $5,000 or imprisonment for not more than six months, or both.

Appeals related to any disciplinary actions resulting from violations of these policies should be taken to the Student Judicial Council (student appeals) or the President's Cabinet (employee appeals).

The Technology Advisory Committee will be responsible to periodically review and revise these policies. Final approval of these policies rests with the President's Cabinet.