

Seattle University Computer Acceptable Use Policy

Revised: December 1997

Approved by Cabinet: December 23, 1997

INTRODUCTION

This document constitutes a University-wide policy for the management of centralized computing resources, computer data networks and stand-alone computers that are owned and administered by Seattle University. This policy reflects the ethical principles of the University community and indicates, in general, what privileges and responsibilities are characteristic of the University computing environment.

This document is intended to give computer users guidelines of what constitutes appropriate and inappropriate use of University computer resources. It also provides guidelines to the system administrators to govern their actions and responsibilities in providing computing resources to the University.

Evidence of illegal activities or policy violations will be turned over to the appropriate authorities as soon as possible after detection. Depending on the nature of the violation, responses including revocation of access, suspension of accounts, University disciplinary action or prosecution to the full extent of the law may be employed.

GENERAL POLICIES

Computer use has become an integral part of many University activities. While much computing can now be done on individual computing resources, most information and communications systems either reside on central computers or use networks.

All computing resources must be used in an ethical and responsible manner. All computing resources provided by the University are intended to further the mission of the University. Equipment, supplies, bandwidth and accounts are to be used for University related work. You are responsible for taking care of all equipment provided by the University and not consuming more than your fair share. All users should be respectful of other users' privacy and needs.

EXISTING UNIVERSITY RULES & REGULATIONS

This policy is intended to be an addition to existing University rules and regulations and does not alter or modify any existing University rule or regulation.

SECURITY

Seattle University will assume that users are aware that electronic files are not entirely secure. Users will be informed of methods available for protecting information on central computing resources from loss, tampering, unauthorized search or other access. Levels of obtainable security will vary depending on the system. Information on procedures appropriate to each resource will be available from the Information Technology Help Desk.

Information Technology will make all reasonable efforts to keep information stored on computing resources and traversing University networks secure from unauthorized access. The level of security desired and required is a decision made by University administrators. Whenever possible, Information Technology will make recommendations when security enhancements are required or available.

Responsibilities of Users

You are 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 of authorization that are assigned to individual users SHOULD NOT be shared with others.

You should assign an obscure account password and change it frequently. (See password guidelines below for help in choosing an obscure password)

You should understand the level of protection each computer system automatically applies to files and supplement it, if necessary, for sensitive information.

The personal computer user should be aware of computer viruses and other destructive computer programs and take steps to avoid being a victim or unwitting distributor of these programs.

You should never leave a terminal or computer unattended without first logging out.

You should not give your login name and password to anyone. You are responsible for all activity occurring from your account.

You are ultimately responsible for resolution of problems related to the invasion of your privacy or loss of data. The University will make every effort to assist you in resolution of any such problem, but do not make the assumption it will just be taken care of without your participation.

CONFIDENTIALITY & PRIVACY

In general, the University will treat information stored on computers as confidential (whether or not that information is protected by the computer system). Requests for disclosure of information will be honored only under one of the following conditions:

- when approved by the appropriate University officials or the head of the department involved;
- when authorized by the owners of the information;
- when required by local, state or federal law.

Requests for disclosure of any information must be made in writing. The request must include explanation of the specific information sought: requests for all information belonging to an individual are not generally required, but will be honored if authorized by the appropriate University official.

In any case involving campus (Public Safety), local, state, or federal law enforcement investigation, the Manager of Public Safety or the Assistant Manager of Public Safety may request and authorize disclosure of information.

Except when inappropriate, computer users will receive notice of such disclosures, including a copy of the written request for disclosure.

Viewing of information in the course of normal system maintenance does not constitute disclosure.

System Administrator Responsibility

System administrators are responsible for the reliable operation of the network and computers. This responsibility includes the authority to examine any information residing on or traversing any University computer resource. System administrators are prohibited from examining any information on any system or network that is not necessary in the performance of their duty.

Any private information viewed by a system administrator in the course of performance of routine responsibilities must not be discussed, disclosed or acted upon unless the information found specifically violates the terms of this policy. Whenever possible the system administrator should inform the user if a file or mail message is read, modified or deleted during system administration and provide a reason why it was necessary to read the file or Email message. Any inappropriate use of this information by a system administrator constitutes a breach of trust between the University and the computer user.

Computer system administrators whose actions violate the terms of this policy are subject to sanctions imposed by the University including possible termination of employment.

Table 1: Definition of Appropriate University Officials

When the individual involved is a:	The appropriate University official is:
Student	Director, Center for Event Planning and Student Activities -or Vice President for Student Development
Staff Member	Assistant Vice President for Human Resources
Faculty Member	Provost -or Dean of School for faculty member

CLASSIFICATION OF COMPUTER-RELATED OFFENSES

This is intended to provide a framework for understanding the severity of offenses (violation of this policy). Offenses not specifically listed in this list will be referred to the appropriate University official for determination of appropriate sanctions.

Violators of computing resources use policies will be subject to the normal disciplinary procedures of the University, including those applicable to students as described in the "Code of Student Conduct." The loss of computing privileges may also result. Violations of the policies described below for legal and ethical use of computing resources will be dealt with in a serious and appropriate manner. Illegal acts involving University computing resources may also be subject to prosecution by local, state or federal authorities.

Level 1 - Nuisance

These offenses generally show a lack of consideration of other computer users, but do not threaten privacy, computer integrity or violate ethical principles. The individual employed poor judgment.

Sanctions:

The user will be issued a verbal, Email or hardcopy warning that their actions were not acceptable. Any repeated level 1 offense will be raised to a level 2 offense.

Level 2 - Questionable Ethics

These offenses often involve violations where the ethics of actions are in question. A person's privacy or computer integrity was violated.

Sanctions:

The user's account or computer access (including access to the computer labs) will be suspended until a formal session with an Information Technology staff member has been attended. A copy of this document will be handed to the user with the specific area of offense highlighted. Any repeated level 2 offense will be raised to a level 3 offense.

Level 3 - Severe

This user has done something that warrants investigation and an incident report by Public Safety.

Sanctions:

The user has committed an offense that warrants investigation and a formal report by Public Safety. The user's account and computer access (including access to the computer labs) will be suspended. The user must attend a session with an Information Technology staff member. The I.S. staff member will contact Public Safety to report the incident. All computer privileges will continue to be suspended until the completion of the investigation and issuance of a report by Public Safety. In most cases the appropriate University official (see Table 1 above) will make the determination if computer privileges are to be returned to the user. Any repeated level 3 offense will be rated to a level 4 offense.

Level 4 - Criminal

A person who commits a level 4 offense is generally under investigation by Public Safety and/or local, state or federal law enforcement.

Sanctions:

Any user committing a level 4 offense forfeits all rights to computer privileges. Any and all information requested by Public Safety, local, state or federal law enforcement will be provided. If the user is found guilty of the offense under investigation, any future access to University computer resources must be first approved by the appropriate University official, and that official may stipulate usage only under supervised circumstances.

Any computer offense not explicitly classified in this document will be handled on a case-by-case basis. The University reserves the right to stiffen or lessen sanctions based on situations involved in the offense.

Any user may initiate a grievance procedure about the application of any policy defined in this document by contacting the appropriate University official.

In most cases Information Technology is involved in the imposition of any sanctions. In cases where the offense is alleged, and not admitted or proven, the matter will be handed over to Public Safety for investigation, and the appropriate University official will make the final determination of sanctions if necessary.

APPROPRIATE AND ACCEPTABLE USE GUIDELINES

Overview

This section contains general guidelines to consider when using University computer systems. After each guideline is a number or a range in parenthesis that corresponds to a level in the "Classification of Computer-Related Offenses" section above.

Institutional Purposes

University computing resources are to be used to advance the University's mission of education. Faculty, staff and students may use them only for purposes related to their studies, their responsibilities for providing instruction, the discharge of their duties as employees, their official business with the University, and other University-sanctioned activities. The use of University computing resources for commercial purposes is permitted only by special arrangements with the appropriate University official or as defined in existing conflict of interest policies.

Legal Guidelines

You are responsible for using all University resources in strict accordance with local, state, and federal laws. These laws cover such areas as illegal access to computer systems, networks, and files; copyright violations; and harassment issues.

Here are some example guidelines that fit this category:

- DO follow the computer usage policy of any system and/or network used for personal or University business. (3)
- DO NOT harass, intimidate, libel or slander other users. (3-4)
- DO observe every user's right to privacy. (3)
- DO NOT continue to send Email, talk requests or messages to any user if that user requests that you remove him/her from the mailing list. Failure to comply may constitute harassment. (2)
- DO NOT steal, destroy or damage equipment, software, or data belonging to the University, other users or other entities on the Internet. (4)

- DO NOT disrupt or monitor electronic communications. (4)
- DO NOT copy and/or use software, images, music or other intellectual property unless you are certain you have the right to do so. (3)
- DO NOT attempt to break into any University computing resource. (3)
- DO NOT use University computing and network resources to attempt to break into any other network or computer systems. (3)
- DO NOT solicit via Email, USENET news or web site any activity against local, state or federal law. (3)
- DO NOT participate in any illegal activities using any University resource. (4)

This is by no means a complete list. If what you are doing is illegal, it is also against this policy. Sanctions will be imposed by at least the university and you will be subject to prosecution to the full extent of the law.

Ethical Use Guidelines

Computing resources should be used in accordance with the ethical standards of the University community.

Here are some example guidelines to help you understand the appropriate ethical use of University resources:

- DO use common sense when using University computing resources. If you are doing something that you would mind having someone looking over your shoulder, you probably should not be doing it. (1)
- DO NOT use computer accounts, access codes, or network identification numbers assigned to others unless authorized to do so. (2)
- DO NOT use computer communications facilities in ways that unnecessarily impede the computing activities of others. Participation in these activities are not only unethical, but may constitute harassment. (2)
- DO NOT use computing facilities for private business purposes unrelated to the mission of the University. (3)
- DO NOT participate in academic dishonesty (plagiarism, cheating). (3)
- DO NOT violate network usage policies and regulations for the University's network, or any other network used from University computing resources. (3)
- DO NOT use computing facilities for any project that promotes or involves prejudice based on race, creed, color, age, national origin, sexual orientation, gender or physical or mental disability. (3)
- DO NOT access clearly confidential information from files that may be inadvertently publicly available. (2)
- DO NOT access confidential information about a person (such as their educational records) without their consent or other authorization. (2)
- DO NOT publish or share confidential information. (2)

Cooperative Use Guidelines

Computing resource users can facilitate computing at the University in many ways. Collegiality demands the practice of cooperative computing.

Here are some examples:

- DO regularly delete unneeded files from your accounts on shared computing resources. (1)
- DO NOT overuse connect time, information storage space, printing facilities or processing capacity. (1)
- DO NOT overuse interactive network utilities (such as UNIX talk command or Internet Relay Chat). (1)
- DO NOT use sounds or visuals that might be disruptive to others. (1)
- DO NOT use departmental or individual computing resources, such as a personal or departmental laser printer or modem for any use not directly related to the mission of the University. (1)
- DO NOT use any Email mailing list for any purpose other than the intended purpose of the list. (1-2)

DO be sensitive to the public nature of shared facilities like computer labs:

- DO follow the posted rules. (1)
- DO take good care of the University's lab equipment. (2)
- DO clean up after yourself when you are finished using a lab computer. (1)
- DO NOT create excessive noise at any time or play games when others are waiting for a workstation. (1)
- DO NOT display on-screen images, sounds or messages that could create an atmosphere of discomfort or harassment of others. (2)
- DO NOT bring food or beverages into the computer lab. (1)
- DO NOT remove or steal any equipment or any piece of any equipment from the computer lab. (4)
- DO NOT lock a workstation or computer. (1)

DO NOT interfere in any way with the work of others using University computing resources. (2)

DO NOT run an Internet Relay Chat 'bot' designed to take exclusive control of an IRC channel. (2)

DO NOT leave an Internet Relay Chat 'bot' running without being present. (2)

DO be ecologically minded when printing. (1)

Personal Use Guidelines

Use of any computer resource provided by the University for strictly personal use is prohibited: computing resources are provided for the sole purpose of advancing the missions of the University.

Electronic mail (Email), USENET news and personal web pages are exempted from this prohibition: Email, USENET news and publishing a home page via the World-Wide-Web may be used for personal use as long as the user complies with all terms of this policy

Internet and Email accounts are provided as a privilege to the University community by the University, and not protected as a right under the First Amendment of the Constitution. The University may at its discretion choose to remove any material from any computer or network system that violate the terms of this policy, or is judged to be in poor taste by the appropriate University official. (See Table 1 above)

Self expression in the form of Email, USENET news posting and web pages is allowed, but the user must insure that the Email, news posting or web page are in good taste: that it is not offensive to the majority of people who view the Email, posting or web page. It is the user's responsibility to clearly state that opinions expressed are the user's sole responsibility, and do not reflect the policies or opinions of the University.

There is a fine line between self-expression and furthering a personal agenda, which is specifically prohibited below. If complaints are received about any Email, news group posting or web pages, they will be reviewed the appropriate University official (see Table 1 above) and the University official will be responsible for making the determination on whether or not to remove the Email, news posting or web page in question. During the time any situation is under review, the account involved may be suspended until the situation is resolved.

Here are some examples of personal use guidelines:

DO NOT use any University computer resource to promote a personal agenda (political, business, religious or other). (3)

DO NOT distribute pornography or other questionable material. If you have a question about whether or not something is questionable, it probably is. (2)

DO NOT attack University policy or personnel. There are established procedures for handling grievances. (2)

DO NOT distribute copyrighted material (software, documents, sounds, pictures) via Email, USENET news or the World-Wide-Web. (3)

DO NOT use University Email distribution lists for personal use. (1)

Email Guidelines

Use good judgment and common sense when using Electronic Mail.

Here are some things to remember when using Email:

DO NOT send any Email to someone who has asked you not to do so. This may constitute harassment, and you will be subject not only to the terms of this policy but local, state and federal laws as well. (4)

DO NOT send frivolous or excessive Email messages to recipients either on or off campus. (1)

DO NOT create, send or forward chain letters (messages that are forwarded many times to people who have not solicited the information). Absolutely DO NOT ever send an Email of this nature to any Email list. Failure to comply may mean immediate and permanent suspension of account privileges. (3)

DO send Email containing warnings or virus alerts to helpdesk@seattleu.edu.

DO NOT send Email containing warnings or virus alerts to other University users. (1)

DO NOT flood another system, network or user account with Email. (3)

DO NOT send unwanted Email that is considered to be "Spam." (2) *Spam - Unwanted, unsolicited Email that is generally considered to be a nuisance mailing. Such Emailing does not serve any legitimate business purpose for Seattle University.*

DO NOT send Email to someone you do not know just because you see them logged in or like their Email address. (1)

DO NOT send Email to individuals or groups who you could not reasonably expect to welcome Email from you. (1)

DO NOT obscure the true identity of the sender of Email or forge Email messages. (3)

DO NOT send sensitive or private information via Email. Email is not a secure communications media. Only send information you would be comfortable discussing in room full of people. (1)

DO NOT send any passwords through the Email system. (1)

DO think before you send an Email message. If you are composing a response to an Email message you have received, do not send anything in an Email message you would not say to a person face-to-face. (1)

Email List Guidelines

It is your responsibility to determine the purpose of an electronic mail list before subscribing or sending messages to that list.

DO NOT send to an Email list any mail that is not consistent with the purpose of the list. If you send messages not relevant to the purpose of the list, you will be viewed as having sent unsolicited Email. (2)

DO NOT harvest Email addresses from another Email list in order to establish your own list. If you would like to form a list whose intended purpose closely matches another list, send an Email to the list inviting members who are interested to subscribe to your list. (1)

DO NOT harvest Email addresses from an institution's directory of user accounts. (2)

DO NOT subscribe anyone to an Email list without his or her permission. (1)

DO regularly communicate (monthly or quarterly) to list of subscribers, both the purpose and rules of use of any list for which you are the designated owner or manager.

DO NOT send an Email message to a list designed to instigate or participate in a 'flame war.' (2)

Bulletin Boards and News Groups Guidelines

Use of these types of computer resources should follow the same guidelines as those outlined above for Email lists.

Copyright Guidelines

Seattle University recognizes and respects copyright laws and insists that its faculty, students and staff follow all applicable copyright laws. In general, every document, image, or sound is copywritten upon creation. The nature of Electronic mail, USENET news and the World-Wide-Web makes it very easy to include copywritten material in your work. When possible, seek permission of the copyright holder before including any material that is not your own in any document. Always pay credit where credit is due.

Here are some copyright guidelines:

DO NOT install any unlicensed software on any University system. (3)

DO seek authorization from the system administrator before installing any personally licensed software on any University computer system. (3)

DO NOT make unauthorized/unlicensed copies of any University-owned software. (3)

System and Network Integrity Guidelines

The University provides computer and network equipment to serve the entire campus community. Every effort has been made to insure the stability, performance and reliability of the entire system. You are responsible to make sure your use of any computing resource does not adversely affect the integrity of the system.

Consider the following network and system integrity guidelines when using any University computer system.

DO be conscious that your actions may affect other users. Respect the interests of other computer users and system managers. (1)

DO report suspected security flaws to helpdesk@seattleu.edu.

DO NOT attempt to test security flaws yourself. (2)

DO NOT attempt to disrupt operation of any system or network. (3)

DO NOT alter data, software, or directories other than your own without proper authorization. (3)

DO NOT probe or connect to any computers without authorization. (2)

DO NOT attempt to gain root or supervisor access on any University system without authorization. (3)

DO NOT use University resources as a leap-off point to try to break into other computer systems. (3)

DO NOT install invasive software, such as worms or viruses, on any University system. (3)

DO NOT install any software of any kind on any computer lab computer without authorization. (2)

Offensive material

There is a large amount of offensive material available from the Internet. (Offensive material is defined as material that will offend the majority of people who view the material) The most common type of offensive material is pornography. The University has neither the resources nor tools to police access to this material. Access to this material is governed by this policy, and an immediate supervisor enforces policy.

Use of any University resource (including the connection to Internet itself) to gain access to material that may be classified as offensive while on the payroll of the University is strictly prohibited unless directly related to teaching or research for the advance of the University's mission.

Use of the University modem pool to download offensive material is considered overuse of a resource, and is completely unrelated to the mission of the University and is therefore prohibited.

Publishing any offensive material from Seattle University computer and network resources is prohibited.

The University's USENET news feed contains a number of newsgroups that contain offensive material. The University does not have the resources to make the determination which USENET newsgroups contain offensive material. It is the responsibility of the user to judge whether material could be deemed offensive.

SYSTEM GUIDELINES

Login Disclaimer

All Seattle University Computer Systems must display the following login disclaimer:

Individuals using this computer system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by system personnel.

In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored.

Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.

Internet Firewall Protection

In general, all computer systems will be protected from the Internet via routing filters in place on the Internet border router. Systems which are available from the Internet will only be made available on a port-by-port basis.

DISCLAIMER

As part of the services available from the Internet, the University provides access to a large number of conferences, lists, bulletin boards, ftp, gopher and web sites. Some of these resources may contain objectionable material. The decision is left to the user whether or not to view or participate in any Internet resource.

For those facilities for which the University has control, the rules of acceptable use described earlier apply.

Seattle University takes no responsibility for the content of those entities over which it has no control. Please be aware of the potentially offensive material found in these archives and use the system with the recognition that the University neither assumes responsibility for, nor endorses, any of the content found within.

PERMISSION TO REPRODUCE

Seattle University grants permission to reproduce and reuse portions or the entire Computer Acceptable Use Policy to the general public with the following terms:

Seattle University is acknowledged as a source of information used in preparing the policy or presentation.

All other Universities whose name appears in the Acknowledgments section below must appear in the policy or presentation.

A copy of any policy based in part or in whole on this document be provided to the University. Seattle University will use these documents to continue to refine this document. If any portion of provided documents is included in this policy, the document will be added to the list of acknowledgments below.

ACKNOWLEDGMENTS

Seattle University's Computer Acceptable Use Policy includes language and content adapted from many other universities. Much of the general format and presentation mimics the "Guidelines for Use of the C&C Computer and Network Resources" document published by the University of Washington Computing and Communications department. That document was based on content adapted from UCLA, Virginia Tech., University of Houston, Rice University, Princeton University, University of Illinois and Ohio State University. Additional content was incorporated into this document from similar documents published by the University of Oregon, Seattle Pacific University, Georgetown University and Creighton University.
