Computer and Network Usage Policy

Authority This Policy was approved by the President.

Policy Statement Users of Stanford network and computer resources have a responsibility to properly use and protect those information resources and to respect the rights of others. This policy provides guidelines for the appropriate use of information technologies.

Policy Purpose The purpose of the Computer and Network Usage Policy is to help ensure an information infrastructure that supports the basic missions of the University in teaching, learning and research. Computers and networks are powerful enabling technologies for accessing and distributing the information and knowledge developed at the University and elsewhere. As such, they are strategic technologies for the current and future needs of the University. Because these technologies leverage each individual's ability to access and copy information from remote sources, users must be mindful of the rights of others to their privacy, intellectual property and other rights. This Usage Policy codifies what is considered appropriate usage of computers and networks with respect to the rights of others. With the privilege to use the information resources of the University come specific responsibilities outlined in this Policy.

Summary Users of University information resources must respect copyrights and licenses, respect the integrity of computer-based information resources, refrain from seeking to gain unauthorized access, and respect the rights of other information resource users. This policy covers the appropriate use of all information resources including computers, networks, and the information contained therein.

Section headings are:

1. POLICY SCOPE AND APPLICABILITY

a. Applicability —This policy is applicable to all University students, faculty and staff and to others granted use of Stanford University information resources. This policy refers to all University information resources whether individually controlled or shared, stand-alone or networked. It applies to all computer and communication facilities owned, leased, operated, or contracted by the University. This includes networking devices, personal digital assistants, telephones, wireless devices, personal computers, workstations, mainframes, minicomputers, and any associated peripherals and software, regardless of whether used for administration, research, teaching or other purposes.

b. Locally Defined and External Conditions of Use — Individual units within the University may define "conditions of use" for information resources under their control. These statements must be consistent with this overall policy but may provide additional detail, guidelines and/or restrictions. Where such "conditions of use" exist, enforcement mechanisms defined therein shall apply. These individual units are responsible for publicizing both the regulations they establish and their policies concerning the authorized and appropriate use of the equipment for which they are responsible. Where use of external networks is involved, policies governing such use also are applicable and must be adhered to.

c. Legal and University Process—The University does not exist in isolation from other communities and jurisdictions and their laws. Under some circumstances, as a result of investigations, subpoena or lawsuits, the University may be required by law to provide electronic or other records or other information related to those records or relating to use of information resources ("information records"). The University may in its reasonable discretion review information records, e.g., for the proper functioning of the University or for internal investigations.

2. POLICIES

a. Copyrights and Licenses — Computer users must respect copyrights and licenses to software, entertainment materials, published and unpublished documents, and any other legally protected digital information.

(1) Copying — Any material protected by copyright must not be copied except as specifically stipulated by the owner of the copyright or otherwise permitted by copyright law. Protected material may not be copied into, from, or by any University facility or system, except pursuant to a valid license or as otherwise permitted by copyright law.

(2) Number of Simultaneous Users — The number and distribution of copies of copyrighted materials must be handled in such a way that the number of simultaneous users in a department does not exceed the number of original copies purchased by that department, unless otherwise stipulated in the purchase contract or as otherwise permitted by copyright law.

(3) Copyrights —All copyrighted information (text, images, icons, programs, video, audio, etc.) retrieved from computer or network resources must be used in conformance with applicable copyright and other law. Copied material must be properly attributed. Plagiarism of digital information is subject to the same sanctions as apply to plagiarism in any other media.

b. Integrity of Information Resources — Computer users must respect the integrity of computer-based information resources.

(1) Modification or Removal of Equipment — Computer users must not attempt to modify or remove computer equipment, software, or peripherals that are owned by others, without proper authorization.

(2) Encroaching on Others' Access and Use — Computer users must not encroach on others' access and use of the University's computers, networks, or other information resources, including digital information. This includes but is not limited to: attempting to access or modify personal, individual or any other University information for which the user is not authorized; attempting to access or modify information systems or other information resources for which the individual is not authorized; sending chain-letters, unsolicited bulk electronic mail either locally or off-campus; printing excess copies of documents, files, data, or programs; running grossly inefficient programs when efficient alternatives are known by the user to be available; unauthorized modification of system facilities, operating systems, or disk partitions; attempting to crash or tie up a University computer, network or other information resource; or otherwise damaging or vandalizing University computing facilities, equipment, software, computer files or other information resources.

(3) Unauthorized or Destructive Programs — Computer users must not intentionally develop or use programs which disrupt other computer or network users or which access private or restricted information or portions of a system and/or damage software or hardware components of a system. Computer users must ensure that they do not use programs or utilities which interfere with other computer users or which modify normally protected or restricted portions of the system or user accounts. Computer users must not use network links for any use other than permitted in network guidelines. The use of any unauthorized or destructive program may result in legal civil action for damages or other punitive action by any injured party, including the University, as well as criminal action.

(4) Academic Pursuits — The University recognizes the value of research on game development, computer security, and the investigation of self-replicating code (e.g., computer viruses and worms). The University may restrict such activities in order to protect University and individual computing environments, but in doing so will take account of legitimate academic pursuits**.**

c. Unauthorized Access — Computer users must refrain from seeking to gain unauthorized access to information resources or enabling unauthorized access.

(1) Abuse of Computing Privileges — Users of University information resources must not access computers, computer software, computer data or information, or networks without proper authorization, or intentionally enable others to do so, regardless of whether the computer, software, data, information, or network in question is owned by the University. For example, abuse of the networks to which the University belongs or the computers at other sites connected to those networks will be treated as an abuse of University computing privileges.

(2) Reporting Problems — Any defects discovered in system accounting or system security must be reported to the appropriate system administrator so that steps can be taken to investigate and resolve the problem.

(3) Password Protection — A computer user who has been authorized to use a password-, or otherwise protected, account may be subject to both civil and criminal liability if the user discloses the password or otherwise makes the account available to others without permission of the system administrator.

d. Usage — Computer users must respect the rights of other computer users. Most University systems provide mechanisms for the protection of private information from examination by others. Attempts to circumvent these mechanisms in order to gain unauthorized access to the system or to another person's information are a violation of University policy and may violate applicable law. Authorized system administrators may access computer users' files at any time for maintenance purposes. System administrators will report suspected unlawful or improper activities to the proper authorities.

(1) Prohibited Use — Use of the University's computers, network or electronic communication facilities (such as electronic mail or instant messaging, or systems with similar functions) to send, view or download fraudulent, harassing, obscene (i.e., pornographic), threatening, or other messages or material that are a violation of applicable law or University policy, such as under circumstances that might contribute to the creation of a hostile academic or work environment, is prohibited.

(2) Mailing Lists—Users must respect the purpose and charters of computer mailing lists (including local or network news groups and bulletin-boards). The user of an electronic mailing list is responsible for determining the purpose of the list before sending messages to or receiving messages from the list. Subscribers to an electronic mailing list will be viewed as having solicited any material delivered by the list as long as that material is consistent with the list's purpose. Persons sending to a mailing list any materials which are not consistent with the list's purpose will be viewed as having sent unsolicited material.

(3) Advertisements — In general, the University's electronic communication facilities should not be used to transmit commercial or personal advertisements, solicitations or promotions (see Commercial Use, below). Some public bulletin boards have been designated for selling items by members of the Stanford community, and may be used appropriately, according to the stated purpose of the list(s).

(4) Information Belonging to Others—Users must not intentionally seek or provide information on, obtain copies of, or modify data files, programs, passwords or other digital materials belonging to other users, without the specific permission of those other users.

(5) Privacy — The Health Insurance Portability and Accountability Act of 1996 (HIPAA) contains standards and rules which govern the treatment of individually identifiable health information. Consult the University Privacy Officer (privacyofficer@stanford.edu) for more information.

e. Political, Personal and Commercial Use — The University is a non-profit, tax-exempt organization and, as such, is subject to specific federal, state and local laws regarding sources of income, political activities, use of property and similar matters. It also is a contractor with government and other entities and thus must assure proper use of property under its control and allocation of overhead and similar costs.

(1) Political Use — University information resources must not be used for partisan political activities where prohibited by federal, state or other applicable laws, and may be used for other political activities only when in compliance with federal, state and other laws and in compliance with applicable University policies.

(2) Personal Use — University information resources should not be used for personal activities not related to appropriate University functions, except in a purely incidental manner.

(3) Commercial Use — University information resources should not be used for commercial purposes, except in a purely incidental manner or except as permitted under other written policies of the University or with the written approval of a University officer having the authority to give such approval. Any such commercial use should be properly related to University activities, take into account proper cost allocations for government and other overhead determinations and provide for appropriate reimbursement to the University for taxes and other costs the University may incur by reason of the commercial use. Users also are reminded that the "EDU" domain on the Internet has rules restricting or prohibiting commercial use, and thus activities not appropriately within the EDU domain and which otherwise are permissible within the University computing resources should use one or more other domains, as appropriate.

3. SYSTEM ADMINISTRATOR RESPONSIBILITIES

While the University Trustees are the legal "owners" or "operators" of all computers and networks purchased or leased with University funds, oversight of any particular system is delegated to the head of a specific subdivision of the University governance structure, such as a Dean, Department Chair, Administrative Department head, or Principal Investigator. For University-owned or leased equipment, that person is the responsible administrator in the sense of the policies in this Guide memo.

The responsible administrator may designate another person to manage the system. This designate is the "system administrator". The system administrator has additional responsibilities to the University as a whole for the system(s) under his/her oversight, regardless of the policies of his/her department or group, and the responsible administrator has the ultimate responsibility for the actions of the system administrator.

a. University Responsibilities — The system administrator should use reasonable efforts:

- To take precautions against theft of or damage to the system components.
- To faithfully execute all hardware and software licensing agreements applicable to the system.
- To treat information about, and information stored by, the system's users in an appropriate manner and to take precautions to protect the security of a system or network and the information contained therein.
- To promulgate information about specific policies and procedures that govern access to and use of the system, and services provided to the users or explicitly not provided. This information should describe the data backup services, if any, offered to the users. A written document given to users or messages posted on the computer system itself shall be considered adequate notice.
- To cooperate with the system administrators of other computer systems or networks, whether within or without the University, to find and correct problems caused on another system by the use of the system under his/her control.

b. Policy Enforcement — Where violations of this policy come to his or her attention, the system administrator is authorized to take reasonable actions to implement and enforce the usage and service policies of the system and to provide for security of the system.

c. Suspension of Privileges — A system administrator may temporarily suspend access privileges if he or she believes it necessary or appropriate to maintain the integrity of the computer system or network.

4. INFORMATION SECURITY OFFICER RESPONSIBILITIES

The University's Information Security Officer or the person designated by the Vice President for Business Affairs and Chief Financial Officer shall be the primary contact for the interpretation, enforcement and monitoring of this policy and the resolution of problems concerning it. Any issues concerning law shall be referred to the Legal Office for advice.

a. Policy Interpretation –-The Information Security Officer shall be responsible for interpretation of this policy, resolution of problems and conflicts with local policies, and special situations.

b. Policy Enforcement –- Where violations of this policy come to his or her attention, the Information Security Officer is authorized to work with the appropriate administrative units to obtain compliance with this policy.

c. Inspection and Monitoring — Only the University's Information Security Officer or designate can authorize the inspection of private data or monitoring of messages (including electronic mail) when there is reasonable cause to suspect improper use of computer or network resources.

5. **CONSEQUENCES OF MISUSE OF COMPUTING PRIVILEGES**

A user of University information resources who is found to have purposely or recklessly violated any of these policies will be subject to disciplinary action up to and including discharge, dismissal, expulsion, and/or legal action.

a. Cooperation Expected — Users, when requested, are expected to cooperate with system administrators in any investigation of system abuse. Users are encouraged to report suspected abuse, especially any damage to or problems with their files. Failure to cooperate may be grounds for cancellation of access privileges, or other disciplinary actions.

b. Corrective Action — If system administrators have persuasive evidence of misuse of computing resources, and if that evidence points to the computing activities or the computer files of an individual, they should pursue one or more of the following steps, as appropriate to protect other users, networks and the computer system.

- Provide notification of the investigation to the University's Information Security Officer or designate, as well as the user's instructor, department or division chair, or supervisor.
- Temporarily suspend or restrict the user's computing privileges during the investigation. A student may appeal such a suspension or restriction and petition for reinstatement of computing privileges through the Dean of Students. A staff member may appeal through applicable dispute resolution procedures. Faculty members may appeal through the Dean of their School.
- With authorization from the University's Information Security Officer or designate, inspect the user's files, diskettes, tapes, and/or other computer-accessible storage media on University owned and operated equipment.
- Refer the matter for possible disciplinary action to the appropriate University unit, i.e., the Dean of Students Office for students, the supervisor for staff, and the Dean of the relevant School for faculty or other teaching or research personnel.

c. Student Honor Code and Fundamental Standard— Unless specifically authorized by a class instructor, all of the following uses of a computer are examples of possible violations of the Honor Code:

- Copying a computer file that contains another student's assignment and submitting it for credit;
- Copying a computer file that contains another student's assignment and using it as a model for one's own work;

- Collaborating on an assignment, sharing the computer files and submitting the shared file, or a modification thereof, as one's individual work.

In addition, student misuse of a computer, network or system may violate the Fundamental Standard. Examples would be, but are not limited to: theft or other abuse of computer time, including unauthorized entry into a file, to use, read, or change the contents; unauthorized use of another person's identification or password; use of computing facilities to send abusive messages; or use of computing facilities to interfere with the work of another student or the work of a faculty or staff member.

For cases involving a student, referring the case to the Judicial Affairs Office is the recommended course of action. This ensures that similar offenses may be considered for similar punishments, from quarter to quarter, year to year, and instructor to instructor. It also allows the detection of repeat offenders.

6. **COGNIZANT OFFICE** — Information Security Office

7. **RELATED POLICIES**

   a. **Student Discipline —** See Student Life/Codes of Conduct/Fundamental Standard/Honor Code

   b. **Staff Discipline —** See Guide Memo 22.15, Corrective Action, http://adminguide.stanford.edu/22_15.pdf

   c. **Faculty Discipline —** See the Statement on Faculty Discipline

   d. **Patents and Copyrights —** See Research Policy Handbook 5.1 and 5.2, http://www.stanford.edu/dept/DoR/rph/

   e. **Partisan Political Activities —** See Guide Memo 15.1, http://adminguide.stanford.edu/15_1.pdf

   f. **Ownership of Documents—**See Research Policy Handbook 5.2, http://www.stanford.edu/dept/DoR/rph/5-2.html, and Guide Memo 15.6, http://adminguide.stanford.edu/15_6.pdf

   g. **Incidental Personal Use --** See Research Policy Handbook 4.1, http://www.stanford.edu/dept/DoR/rph/4-1.html, and Guide Memo 15.2, http://adminguide.stanford.edu/15_2.pdf