Stanford
Published in the Administrative Guide

6.2.1 COMPUTER AND NETWORK USAGE POLICY

Last updated on: 03/14/2014
Formerly Known As Policy Number: 62
This policy covers the appropriate use of all information resources including computers, networks, and the information contained therein.

Authority:
Approved by the Vice President for Business Affairs and Chief Financial Officer.

Applicability:
Applies to all University students, faculty and staff, and all others using computer and communication technologies, including the University's network, whether personally or University owned, which access, transmit or store University or student information.

Policy Statement:
Use of Stanford's network and computer resources should support the basic missions of the University in teaching, learning and research. Users of Stanford's network and computer resources ("users") are responsible to properly use and protect information resources and to respect the rights of others. This policy provides guidelines for the appropriate use of information resources.

1. Definitions

As used in this policy:
a. "Information resources" are all computer and communication devices and other technologies which access, store or transmit University or student information.
b. "Information" includes both University and student information.
c. "Personally owned resources" are information resources that are under the control of University employees or agents and are not wholly owned by the University.

2. Policies

a. General Policy
Users of information resources must protect (i) their online identity from use by another individual, (ii) the integrity of information resources, and (iii) the privacy of electronic information. In addition, users must refrain from seeking to gain unauthorized access, honor all copyrights and licenses and respect the rights of other users of information resources.

b. Access
Users must refrain from seeking to gain unauthorized access to information resources or enabling unauthorized access. Attempts to gain unauthorized access to a system or to another person's information are a violation of University policy and may also violate applicable law, potentially subjecting the user to both civil and criminal liability. However, authorized system administrators may access information resources, but only for a legitimate operational purpose and only the minimum access required to accomplish this legitimate operational purpose.

(1) Prohibition against Sharing Identities
Sharing an online identity (user ID and password or other authenticator such as a token or certificate) violates University policy.
(2) 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.
(3) Abuse of Computing Privileges
Users of 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.

c. Usage
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. Use of the University's information resources must comply with University policies and legal obligations (including licenses and contracts), and all federal and state laws.

(1) Prohibited Use
Users must not 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. In particular, contributing to the creation of a hostile academic or work environment is prohibited.
(2) Copyrights and Licenses
Users must not violate copyright law and must respect licenses to copyrighted materials. For the avoidance of doubt, unlawful file-sharing using the University's information resources is a violation of this policy.
(3) Social Media
Users must respect the purpose of and abide by the terms of use of online media forums, including social networking websites, mailing lists, chat rooms and blogs.
(4) 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.
(5) Personal Use
University information resources should not be used for activities unrelated to appropriate University functions, except in a purely incidental manner.
(6) Commercial Use
University information resources should not be used for commercial purposes, including advertisements, solicitations, promotions or other commercial messages, except as permitted under University policy. Any such permitted 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. The University's Chief Financial Officer and Vice President for Business Affairs will determine permitted commercial uses.
(7) Use of University Information
Users must abide by applicable data storage and transmission policies, including Admin Guide 6.3.1 (Information Security). Consult the University Privacy Officer (privacyofficer@stanford.edu [1]) for more information.

d. Personally Owned Resources
Stanford does not require personnel to use their personally owned resources to conduct University business. Individual units within the University may permit such use, and users may choose to use their own resources accordingly. Any personally owned resources used for University business are subject to this policy and must comply with all Stanford requirements pertaining to that type of resource and to the type of data involved. The resources must also comply with any additional requirements (including security controls for encryption, patching and backup) specific to the particular University functions for which they are used.

e. Integrity of Information Resources
Users must respect the integrity of information and information resources.

(1) Modification or Removal of Information or Information Resources
Unless they have proper authorization, users must not attempt to modify or remove information or information resources that are owned or used by others.
(2) Other Prohibited Activities
Users must not encroach, disrupt or otherwise interfere with access or use of the University's information or information resources. For the avoidance of doubt, without express permission, users must not give away University information or send bulk unsolicited email. In addition, users must not engage in other activities that damage, vandalize or otherwise compromise the integrity of University information or information resources.
(3) Academic Pursuits
The University recognizes the value of legitimate research projects undertaken by faculty and students under faculty supervision. The University may restrict such activities in order to protect University and individual information and information resources, but in doing so will take into account legitimate academic pursuits.

f. 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 restrictions, and/or enforcement mechanisms. Where such conditions of use exist, the individual units are responsible for publicizing and enforcing both the conditions of use and this policy. Where use of external networks is involved, policies governing such use also are applicable and must be followed.

g. Access for Legal and University Processes
Under some circumstances, as a result of investigations, subpoenas or lawsuits, the University may be required by law to provide electronic or other records, or information related to those records or relating to use of information resources, ("information records") to third parties. Additionally, the University may in its reasonable discretion review information records, e.g., for the proper functioning of the University, in connection with investigations or audits, or to protect the safety of individuals or the Stanford community. The University may also permit reasonable access to data to third-party service providers in order to provide, maintain or improve services to the University. Accordingly, users of University information resources do not have a reasonable expectation of privacy when using the University's information resources.

3. Oversight of Information Resources

Responsibility for, and management and operation of, information resources is delegated to the head of a specific subdivision of the University governance structure ("department"), such as a Dean, Department Chair, Administrative Department head, or Principal Investigator ("lead"). This person will be responsible for compliance with all University policies relating to the use of information resources owned, used or otherwise residing in their department.

The lead may designate another person to manage and operate the system, but responsibility for information resources remains with the lead. This designate is the "system administrator."

The system administrator is responsible for managing and operating information resources under their oversight in compliance with University and department policies, including accessing information resources necessary to maintain operation of the systems under the care of the system administrator. (See also section 4.b; system administrators should defer to the Information Security Office for access beyond that necessary to maintain operation of the system.)

a. Responsibilities
The system administrator should:

- Take all appropriate actions to protect the security of information and information resources. Applicable guidelines are found at http://securecomputing.stanford.edu [2].
- Take precautions against theft of or damage to information resources.
- Faithfully execute all licensing agreements applicable to information resources.
- Communicate this policy, and other applicable information use, security and privacy policies and procedures to their information resource users.
- Cooperate with the Information Security Office to find and correct problems caused by the use of the system under their control.

b. Suspension of Privileges
System administrators may temporarily suspend access to information resources if they believe it is necessary or appropriate to maintain the integrity of the information resources under their oversight.

4. Reporting or Investigating Violations or University Concerns

a. Reporting Violations
System users will report violations of this policy to the Information Security Office, and will immediately report defects in system accounting, concerns with system security, or suspected unlawful or improper system activities to the Information Security Office during normal business hours and the Office of the General Counsel emergency after-hours phone line at other times.

b. Accessing Information & Systems
Inspecting and monitoring information and information resources may be required for the purposes of enforcing this policy, conducting University investigations or audits, ensuring the safety of an individual or the University community, complying with law or ensuring proper operation of information resources. Only the University's Chief Information Security Officer (or designate) may authorize this inspection and monitoring.

c. Cooperation Expected
Information resource users are expected to cooperate with any investigation of policy abuse. Failure to cooperate may be grounds for cancellation of access privileges, or other disciplinary actions.

5. Consequences of Misuse of Information Resources

A user found to have violated this policy may also have violated the University Code of Conduct, the Fundamental Standard, the Student Honor Code, and/or other University policies, and will be subject to appropriate disciplinary action up to and including discharge, dismissal, expulsion, and/or legal action. The Chief Information Security Officer

will refer violations to University units, i.e., Student Affairs for students, the supervisor for staff, and the Dean of the relevant School for faculty or other teaching or research personnel, if appropriate.

6. Cognizant Office

University's Chief Information Security Officer, or other person designated by the Vice President for Business Affairs and Chief Financial Officer, shall be the primary contact for the interpretation, monitoring and enforcement of this policy.

7. Related Policies

a. Student Discipline—See Student Life/Codes of Conduct/Fundamental Standard/Honor Code
b. Staff Discipline—See Guide Memo 2.1.16 [3]: Addressing Conduct & Performance Issues
c. Faculty Discipline—See the Statement on Faculty Discipline in the Faculty Handbook
d. Patents and Copyrights—See Research Policy Handbook 9.1 [4]and 9.2 [5]; see also the Stanford University Copyright Reminder [6]
e. Political Activities—See Guide Memo 1.5.1 [7]: Political Activities
f. Ownership of Documents—See Research Policy Handbook 9.2 [5] and Guide Memo 1.5.5 [8]: Ownership of Documents
g. Incidental Personal Use—See Research Policy Handbook 4.1 [9], and Guide Memo 1.5.2 [10]: Staff Policy on Conflict of Commitment and Interest
h. Security of Information—See Guide Memo 6.6.1 [11]: Information Security Incident Response
i. Privacy and Security of Health Information (HIPAA)—See Guide Memo 1.6.2 [12]: Privacy and Security of Health Information
j. Data Classification, Access and Transmittal and Storage Guidelines—See http://dataclass.stanford.edu [13].
k. Endpoint Compliance—See http://securecomputing.stanford.edu/endpoint_compliance.html [14]
l. **Accessibility of Electronic Content**—See https://adminguide.stanford.edu/chapter-6/subchapter-8/policy-6-8-1 [15]

Links
[1] mailto:privacyofficer@stanford.edu?subject=Information
[2] http://securecomputing.stanford.edu
[3] https://adminguide.stanford.edu/2-1-16
[4] http://doresearch.stanford.edu/policies/research-policy-handbook/intellectual-property/inventions-patents-and-licensing
[5] http://doresearch.stanford.edu/policies/research-policy-handbook/intellectual-property/copyright-policy
[6] http://library.stanford.edu/using/copyright-reminder
[7] https://adminguide.stanford.edu/1-5-1
[8] https://adminguide.stanford.edu/chapter-1/subchapter-5/policy-1-5-5
[9] https://doresearch.stanford.edu/policies/research-policy-handbook/conflicts-commitment-and-interest/faculty-policy-conflict-commitment-and-interest
[10] https://adminguide.stanford.edu/1-5-2
[11] https://adminguide.stanford.edu/6-6-1

[12] https://adminguide.stanford.edu/1-6-2
[13] http://dataclass.stanford.edu
[14] https://itservices.stanford.edu/guide/endpoint-compliance
[15] https://adminguide.stanford.edu/chapter-6/subchapter-8/policy-6-8-1