Chicago State University Computer Usage Policy

INTRODUCTION

This policy defines the boundaries of acceptable use of Chicago State University computing and communication resources, including computers, data storage systems, mobile devices, electronic data, networks, electronic mail services, electronic information sources, voice mail, telephone services, and other communication resources. In addition, this policy reflects the goal of CSU to foster academic freedom while respecting the principles of freedom of speech and the privacy rights of CSU students, faculty, employees, courtesy affiliates, and guests.

CSU's computing and communication resources are the property of CSU. They are to be used for the advancement of CSU's educational, research, service, community outreach, administrative, and business purposes. Computing and communication resources are provided for the use of faculty, staff, currently admitted or enrolled students, and other properly authorized users. When a user's affiliation with CSU ends, CSU will terminate access to computing and communications resources and accounts. CSU may, at its discretion, permit the user to have access to accounts and e-mail forwarded or redirected for a limited period of time.

The Information Technology Department (ITD) is responsible for the maintenance and security of CSU's central computing and communications resources. This includes recommendations for effective practices by its users, which include faculty, staff, students, and affiliates. This policy is designed to aid the university community in protecting the confidentiality, availability, and integrity of university information resources.

Users of CSU's computing and communications resources are required to comply with this policy, other applicable CSU and Chicago Board of Trustees policies, and state and federal laws. When necessary, enforcement will be consistent with other applicable CSU administrative policies and procedures.

REQUIREMENTS AND PROHIBITED USES

Requirements for the Use of CSU Computing and Communications Resources

1. Users must comply with all applicable local, state, and federal laws and regulations, and with CSU and Board of Trustee policies.
2. Users must respect academic freedom and free speech rights.
3. Users must be truthful and accurate in personal and computer identification.
4. Users must respect the rights and privacy of others, including intellectual property and personal property rights.
5. Users must not compromise the integrity of electronic networks, must avoid restricted areas, and must refrain from activities that may damage the network, or transmitted or stored data.

6. Users and individuals responsible for system administration must maintain the security of accounts and are required to protect and regularly change their account passwords according to standards maintained by ITD.
7. Users, once aware of a security concern, must notify ITD of information security concerns including, but not limited to, breaches of sensitive data or compromised accounts.
8. Users are responsible for the protection, security, and integrity of university data and resources under their control according to the standards maintained by ITD.

Prohibited Uses of CSU Computing and Communications Resources

1. Unlawful communications, including threats of violence, obscenity, child pornography, and harassing communications, are prohibited.
2. Use of CSU computer resources for private business or commercial activities, or for fund-raising or advertising on behalf of non-CSU organizations, is prohibited.
3. The unauthorized reselling of CSU computer resources is prohibited.
4. Unauthorized use of university trademarks or logos and other protected trademarks and logos is prohibited.
5. CSU Web pages may link to commercial Web sites, but any link that generates, or has the potential to generate, revenue to CSU or to any individual or company, including click trade or banner advertising, must be approved by Purchasing and Finance.
6. College and department Web sites may include links to commercial Web sites to provide information related to the mission or function of the college or academic or administrative unit. Any link that generates, or has the potential to generate, revenue to the college or academic or administrative unit must be approved through Purchasing and Finance.
7. Any alteration of addresses, uniform resource locator (URL), or other action that masks the csu.edu domain as a host site is prohibited unless authorized by ITD.
8. Unauthorized anonymous and/or pseudonymous communications are prohibited. All users are required to cooperate with appropriate CSU personnel or other authorized personnel when investigating the source of anonymous messages.
9. Misrepresenting or forging the identity of the sender or the source of an electronic communication is prohibited.
10. Unauthorized attempts to acquire and use passwords of others are prohibited.
11. Unauthorized use and attempts to use the computer accounts of others are prohibited.
12. Altering the content of a message originating from another person or computer with intent to deceive is prohibited.
13. Unauthorized modification or deletion of another person's files, account, or news group postings is prohibited.
14. Use of CSU computer resources or electronic information without authorization or beyond one's level of authorization is prohibited.
15. Interception or attempted interception of communications by parties not authorized or intended to receive them is prohibited.
16. Making CSU computing resources available to individuals not affiliated with CSU without approval of an authorized CSU official at or above the level of dean/university librarian or director is prohibited.

17. Compromising the privacy or security of electronic information is prohibited.
18. Infringing upon the copyright, trademark, patent, or other intellectual property rights of others in computer programs or electronic information (including plagiarism and unauthorized use or reproduction) is prohibited. The unauthorized storing, copying, or use of audio files, images, graphics, computer software, data sets, bibliographic records, and other protected property is prohibited except as permitted by law.
19. Interference with or disruption of the computer or network accounts, services, or equipment of others is prohibited.
20. The propagation of computer "worms" and "viruses," the sending of electronic chain mail, denial of service attacks, and inappropriate "broadcasting" of messages to large numbers of individuals or hosts are prohibited.
21. Failure to comply with requests from appropriate CSU officials to discontinue activities that threaten the operation or integrity of computers, systems, or networks, or that otherwise violate this policy is prohibited.
22. Revealing passwords or otherwise permitting the use by others (by intent or negligence) of personal accounts for computer and network access without authorization is prohibited.
23. Altering or attempting to alter files or systems without authorization is prohibited.
24. Scanning of networks, networked devices, or applications for security vulnerabilities without specific authorization by the ITD is prohibited.
25. Attempting to alter or connect any computing or networking components (including, but not limited to, bridges, routers, DHCP servers, wireless access points, and hubs) on the CSU network without approval of the ITD is prohibited.
26. Installation or alteration of wiring, including attempts to create network connections, or any extension or retransmission of any computer or network services without the approval of the ITD is prohibited.
27. Conduct leading to disruption of electronic networks or information systems is prohibited.
28. Conduct leading to the damage of CSU electronic information/data, computing/networking equipment, and resources is prohibited.

Prohibited Access

CSU may restrict access from within its network to any sites in furtherance of this policy. A user may contact ITD to request access to a restricted site or to report that a site was restricted in error.

INFORMATION POSTED TO CSU COMPUTERS OR WEB PAGES

Restriction on Use of CSU Web Pages

CSU Web pages may be used only for CSU business and only authorized individuals may modify or post materials to these pages. No other pages may suggest that they are university Web pages. If confusion is possible, pages should contain a disclaimer and links to CSU sites.

Responsibilities of Individuals Posting Materials

By posting materials and using CSU computing facilities, the user represents that he or she has created the materials or that he or she has the right to post or use the materials. The storage, posting, or transmission of materials must not violate the rights of any third person in the materials, including copyright, trademark, patent, trade secrets, and any rights of publicity or privacy of any person. The materials posted must not be defamatory, libelous, slanderous, or obscene.

Prohibition against Commercial Use

The site may not be used for unauthorized commercial purposes.

University Control of CSU Web Pages

The use of the site is at the sole discretion of CSU. CSU does not guarantee that the user will have continued or uninterrupted access to the site. The site may be removed or discontinued at any time at the discretion of CSU in accordance with CSU policy, or as needed to maintain the continued operation or integrity of CSU facilities.

CSU makes reasonable efforts to protect the integrity of the network and related services, but CSU cannot guarantee backup, disaster recovery, or user access to information posted on personal computers or Web pages.

Access to services and file storage may be approved for emeriti, retired staff, alumni, and guests.

ELECTRONIC MAIL AND ELECTRONIC COMMUNICATIONS

Conditions for Restriction of Access to Electronic Mail

Access to CSU e-mail is a privilege that may be wholly or partially restricted without prior notice and without consent of the user:

1. if required by applicable law or policy
2. if a reasonable suspicion exists that there has been or may be a violation of law, regulation, or policy

or

3. if required to protect the integrity or operation of the e-mail system or computing resources or when the resources are required for more critical tasks as determined by appropriate management authority.

Access to the e-mail system may require approval of the appropriate CSU supervisory or management authority (e.g., department head, system administrator, etc.).

Conditions for Permitting Inspection, Monitoring, or Disclosure

CSU may permit the inspection, monitoring, or disclosure of e-mail, computer files, and network transmissions when:

1. required or permitted by law, including public records law, or by subpoena or court order
2. CSU or its designated agent reasonably believes that a violation of law or policy has occurred

or

3. necessary to monitor and preserve the functioning and integrity of the e-mail system or computer systems or facilities.

All computer users agree to cooperate and comply with CSU requests for access to and copies of e-mail messages or data when access or disclosure is authorized by this policy or required or allowed by law or other applicable policies.

CSU Responsibility to Inform of Unauthorized Access or Disclosure

If CSU believes unauthorized access to or disclosure of information has occurred or will occur, CSU will make reasonable efforts to inform the affected computer account holder, except when notification is impractical or when notification would be detrimental to an investigation of a violation of law or policy.

Prohibition against Activities Placing Strain on Facilities

Activities that may strain the e-mail or network facilities more than can be reasonably expected are in violation of this policy. These activities include, but are not limited to: sending chain letters; “spam,” or the widespread dissemination of unsolicited e-mail; and “letter bombs” to resend the same e-mail repeatedly to one or more recipients.

Confidentiality

Confidentiality of e-mail and other network transmissions cannot be assured. Therefore all users should exercise caution when sending personal, financial, confidential, or sensitive information by e-mail or over the network.

Electronic Information as Illinois Public Record

Most electronic information (e.g., e-mail) produced in the course of university business is considered an Illinois public record, and must be stored or deleted in accordance with Illinois public records law. Consult with the university archivist for guidance on procedures for external storage or deletion of public records.

Right to Examine Computers and Equipment

University-owned computers and equipment may be examined to detect illegal content and to evaluate the security of the network. Networks, networked devices, and applications may be scanned for vulnerabilities as authorized by the ITD.