Chicago State University Computer Usage Policy

Introduction

This document provides guidelines for appropriate use by students, faculty and staff of computers, and other technological facilities and services at Chicago State University. It is not a comprehensive document covering all aspects of computer and technology use. It offers principles to help guide members of the Chicago State University community, and specific policy statements that serve as a reference points.

This policy will be modified as new questions and situations arise. Each individual who uses Chicago State University's computing facilities thereby agrees that his/her use of these facilities will remain within the bound of acceptable use as described in this and other University computing policies or other Chicago State University codes of conduct.

Technology is an enormously rich resource for innovation in the furtherance of Chicago State University's academic mission. It also offers new forums for the University's historic commitment to the expression and discussion of a wide diversity of ideas and opinions. But technology also increases the risks of actions, deliberate or not, that are harmful in various ways, including: (a) interference with the privacy rights of others; (b) violation of the law; (c) interference with the mission of the University; or (d) endangering the integrity of the University's information computer systems, network or other technologies.

The proliferation of computers and information technologies does not alter basic codes of behavior in academic life, but, it does place some issues in new contexts. Chicago State University computing systems and resources shall be used only for legitimate University purposes, including instruction, research, administration, public information and service and other approved tasks.

Technology has greatly expanded our ability to access and exchange information. The use of technology therefore, requires more vigilant efforts and more secure safeguards to protect both property and privacy rights.

The guidelines that follow seek to both preserve the freedom to inquire and share information and sustain the security and integrity of individuals within the community, computers and the network system itself. While some of the guidelines call for respectful and responsible use of the computer networks to protect the rights of individuals, others warn against actions that may violate the law.

Responsibilities

All computers, network or other technology users have the responsibility to use CSU technology resources in an ethical and lawful manner. User should:

1. Know and understand CSU's Computer Use Policy.

2. Abide by CSU policy on ownership and responsibility for CSU websites, copyright, intellectual property and fair use.
3. Maintain their own files, save and back up all data, and remove outdated materials from network storage.
4. Protect the integrity of their accounts by changing passwords regularly, not giving passwords to any other person, or not leaving a networked computer without logging out.
5. Learn how to operate the hardware and software the user has.

Principles and Guidelines:

Use of CSU's computers, networks and other technologies are privileges.

CSU may restrict students, staff, faculty or other authorized users who:

1. Enter**s** and University any computer, computing network, server or system which is unauthorized.
2. Engages in any activity that violates the integrity or interferes with the normal operation of the University's computing system.
3. Uses and "peer to peer" software that violates digital rights management. The use of any "peer to peer" software that violates digital rights management is strictly prohibited.
4. Makes an unauthorized access of the University's computing system by:
    - Any use of another person's identification and password;
    - Unauthorized use of another person's device for accessing the network or other systems;
    - Unauthorized entry into another person's device or system files to read or change a file's content;
5. Any activity which causes a denial of service upon University computing resources.
6. Any activity which launches a denial of service upon any other website.
7. Any activity that interferes with the work of another CSU student, faculty member, staff member or University official.
8. Any use for personal gain or commercial activity.
9. Any activity which is illegal under Federal or State law, including but not limited to:
    - Accessing child pornography
    - Participation in chain letters
    - Introduction of malware or other hacker activity
    - Unauthorized reproduction or distribution of copyrighted material including software, text images, audio or video
    - Installation of software which is not licensed for use on the machine where it is installed.

Compliance with the Computer Use Policy Means:

1. **Respect the rights and sensibilities of others.**
   a. Electronic mail and all other electronic communication (including websites and blog posts on the university server) should adhere to the University standards of conduct which prohibit any communication which tends to embarrass or humiliate any member of the community. Respect others you contact electronically by avoiding lewd, obscene, defamatory or harassing comments.
   b. Others have a right to know who is contacting them.
   c. Respect the privacy of others and their accounts. Do not access or intercept files or data of others without permission. Do not use the password of others or access files under false identity.
   d. Distribution of excessive amounts of unsolicited mail is inappropriate.
   e. While the University encourages respect for the rights and sensibilities of others, it cannot protect individuals against the existence or receipt of materials that may be offensive to them. Those who make use of electronic communications may come across or be recipients of material they find offensive or simply annoying.

2. **Be aware of the legal implications of your computer use.**
   a. The Internet enables users to disseminate material worldwide. Thus the impact of dissemination on the internet is often far broader than that of a statement made on paper or in routine conversation.
   b. Much of what appears on the internet is protected by copyright law regardless of whether the copyright is expressly noted. Users should generally assume that material is copyrighted unless they know otherwise and not copy or disseminate copyrighted material without permission. Copyright protection also applies to much software, which is often licensed to the University with specific limitations on its use. Both individual users and the University may, in some circumstances, be held legally responsible for violations of copyright.
   c. Many other state and federal laws, including those prohibiting deceptive advertising, use of others' trademarks, defamation, violations of privacy, and obscenity apply to network-based communications.

3. **Respect the mission of the University in the larger community**
   a. The University makes internet resources available to students, faculty and staff to further the University's educational, research, service and University-related activities and missions. Recognizing that the Internet is also an integral part of socialization and leisure among students living on campus, the network is available to students for purposes of non-academic communications and entertainment to the extent that such use does not compromise the network or the amount of bandwidth available for academic-related uses.
   b. The University does not monitor the content of web pages, electronic mail or other on-line communications and is not responsible for the views expressed by individual users. Under certain circumstances, however, the University may be held liable if it fails to take reasonable remedial steps after it learns of illegal uses of its computer facilities. Use computer resources lawfully.

c. Remember that you are responsible for all activity involving your account. Keep your account secure and private. Do not use identifying data or common words as a password; your password should be difficult to crack or otherwise guess either by individuals or by sophisticated computer programs.

d. The University is the custodian of a wide array of personal and financial data concerning its students, staff, faculty and patients, as well as the University itself. Respect the University obligations of confidentiality as well as your own. Only those with authorization may access, communicate or use confidential information.

e. Material posted on web pages is generally accessible and thus deserves even greater thought and care than your private electronic mail. Remember that, absent restrictions, your web page is available to anyone, anywhere, and act accordingly.

f. The University has a right to expect that computer users will properly identify themselves. Computer accounts are assigned and identified to individuals. Don't misrepresent yourself.

4. **Do not harm the integrity of the University's computer systems and networks.**

a. Today's information technology is a shared resource. Respect the needs of others when using computer and network resources. Do not tamper with facilities and avoid any actions that interfere with the normal operations of computers, networks, and facilities.

b. Avoid excessive use of computer resources. They are finite and others deserve their share. "Spamming" and similar inappropriate uses of University resources are not acceptable. Web pages that are accessed to an excessive degree can be a drain on computer resources and, except where significant to the University's mission, may require the University to ask that they be moved to a private Internet provider.

c. Although a respect for privacy is fundamental to the University's policies, understand that almost any information can in principle be read or copied; that some user information is maintained in system logs as a part of responsible computer system maintenance; that the University must reserve the right to examine computer files, and that, in rare circumstances, the University may be compelled by law or policy to examine even personal and confidential information maintained on University computing facilities.

d. You are granted privileges and responsibilities with your account. While these vary between groups, the use of University resources for personal commercial gain or for partisan political purposes (not including the expression of personal political views, debate and the like) is inappropriate and possibly illegal.

e. Individual University computer systems have varying resources and demands. Some have additional and sometimes more restrictive guidelines applicable to their own user.

Implementation

A. All University codes of conduct apply to information technology as well as to other forms of communication and activity.
B. Systems managers or other individuals within an academic or administrative unit may be empowered to suspend some or all privileges associated with computer use in cases of misuse or threat to the integrity of all or part of the University's information management resources.
C. Before any permanent action is taken against a user, the user will be advised of the bases for the proposed action and given an opportunity to respond. Concerns about such actions may be raised through the usual administrative or academic channels associated with the dean, school, facility or resource in question.
D. Where a violation of University policies or applicable law appears to warrant action beyond a suspension or elimination of computer privileges, the matter may be referred to a supervisor, administrator or University disciplinary body with appropriate authority or to law enforcement authorities.
E. Complaints or concerns about another's use of University computer resources should be directed to the administrator responsible for the facility or resource in question.
F. If you have any questions regarding proper computer usage contact your ethics officer at ethics@csu.edu.
G. If you have any technical issues regarding the use of your computer, software, server or other network services contact ITD at helpdesk@csu.edu.

I certify that I have carefully read and reviewed the content of the

2013 ANNUAL COMPUTER USE POLICY

Furthermore, I certify that I understand my failure to comply with the laws, rules, policies, and procedures referred to within this training course may result in disciplinary action up to and including termination of University employment and possible criminal prosecution, depending on the nature of the violation.

Name: _____

(Print: last name, first name, middle initial)

Signature: _____

(Not Valid Without Signature)

Today's Date: _____

Date of Birth: _____

(mm/dd)

UID: _____

To be properly credited for participating in computer use training, please complete and return the signature page to the Chicago State University Office of Human Resources:

Office of Human Resources
Chicago State University
9501 South King Drive, ADM 203
Chicago, IL 60628