East Los Angeles Community College

Library Theft Policy (Crime Against Property)
"A person employed by a library facility may detain a person for a reasonable time for the purpose of conducting an investigation in a reasonable manner whenever the person employed by a library facility has probable cause to believe the person to be detained is attempting to unlawfully remove or has unlawfully removed books or library materials from the premises of the library facility." (CALIFORNIA PENAL CODE SECTION 490.5 (f)(1))." "IN ORDER TO PREVENT THE THEFT OF BOOKS AND LIBRARY MATERIALS, STATE LAW AUTHORIZES THE DETENTION FOR A REASONABLE PERIOD OF ANY PERSON USING THESE FACILITIES SUSPECTED OF COMMITTING "LIBRARY THEFT" (PENAL CODE SECTION 490.5)."

Computer Use Policy

- Two hour use for research stations
- "first come, first served" basis for Internet lab computers
- No chat rooms or IRC (Internet relay chat)
- Games prohibited
- Obscene materials prohibited
- Anyone apprehended viewing obscene materials using a library computer will have their library privileges suspended
- Use of personal software prohibited

Los Angeles Harbor College

RULES OF OPERATION:
These policies are necessary to maintain a pleasant and workable study environment and to assure the longevity of our instructional materials and equipment.
. Students must adhere to District and College Conduct and Computing Facilities Policy.
. When using lab services, students must log in and out of the center on the computer tracking system.
. Students need a current, valid LAHC Registration Fee Receipt to access materials in the LAC.
. No food or drink, except water is allowed in the LAC.
. Children are not allowed in the LAC.
. Instructional materials may not be taken out of the LAC.
. The LAC maintains a quiet study hall atmosphere – turn off pagers, cell phones, pods, etc.
. Do not write or mark in any of the materials on loan to you.
. Students not being tutored may sit at tutoring tables only with permission of the tutor coordinator.
. Printing is limited to 15 pages per day.
. Copiers are available in the Library and Seahawk Center.

. Students can get regular tutoring for classes that they are currently enrolled in at Los Angeles Harbor College.
. Report broken, damaged, or defected equipment and deflecting materials immediately.
. If a fire alarm sounds, gather your belonging and LEAVE THE BUILDING BY DESIGNATED EXITS AND WAIT OUTSIDE AT LEAST 50 FEET FROM THE BUILDING UNTIL THE ALL CLEAR SIGNAL RINGS.

Los Angeles Mission College

Policy
This policy outlines the acceptable use of Los Angeles Mission College's computer and network resources by faculty and staff. Users of computing resources are expected to take a responsible and professional approach to the use of these resources, as access to these resources is a privilege not a right. The College's computing resources and facilities are intended for instructional and administrative use; computing facilities and network access cannot be used for commercial purposes without proper written authorization. While there may be incidental personal use of College technology resources, this type of use must adhere to all College acceptable use policies and procedures. Employees' supervisors may restrict personal activities of their employees if these personal activities are impacting the employees' job performances.

Members of the user community must use only those resources to which they have been specifically granted access by the College; and by using the College's technology resources, users assume personal responsibility for their appropriate use and agree to comply with this policy and other applicable College policies, as well as city, state, and federal laws and regulations.

In making acceptable use of resources you are expected to:
- use resources only for authorized purposes;
- protect your user ID, password, and system from unauthorized use;
- access only information that is your own, that is publicly available, or to which you have been given authorized access;
- be considerate in your use of shared resources;
- demonstrate respect for principles of open expression;
- be aware of copyright laws as they apply to computer software and other materials that you may access with College computing resources.

Unacceptable use of resources may include but is not limited to:

- use of another person's system, user ID, password, files, or data, or giving the use of one's system, user ID, password, files, or data;
- engage in any activity that might be purposefully harmful to systems, resources, or data, such as creating or propagating viruses, disrupting services, or attempting to gain unauthorized access to resources or data;
- make or use illegal copies of copyrighted materials, software, or music, store such copies on College systems, or transmit them over College networks;
- creation, display, or distribution of defamatory or harassing material, which is in violation of existing law or College policy;
- use of College system for any other illegal activity;
- monopolizing systems, overloading networks with excessive data, or wasting college resources;
- use the College's equipment or networks for personal profit;
- unauthorized installation of hardware or software onto any College owned computer/network (the Information Technology Department is responsible for all installations, requests for exceptions should be sent to the Information Technology Help Desk).

Privacy and Use of Information:
Employees are expected to be knowledgeable of, and to perform their duties in compliance with, federal, state, and local laws and college policies, including the provisions of the Family Educational Rights and Privacy Act and Health Insurance Portability and Accountability Act designed to protect the confidentiality of data and the privacy of individuals. Confidential or demographic data that pertains to students, employees, or college operations, must be used in a manner that protects rights of privacy and limits personal and institutional liability.

Consequences:
Employees of the College who violate this policy are subject to disciplinary action up to and including termination of their employment. The College also reserves the right to withdraw access to its system to any user. The College, additionally, reserves the right to notify appropriate legal authorities in the event that its system is used in a manner that constitutes a violation of any local, state, or federal law.

Information Disclaimer:
The College is not responsible for the loss of information or interruption of electronic communications. The College reserves the right to discard incoming mass mailings ("spam") without notifying the sender or intended recipient and to block all Internet communications from sites that are involved in extensive spamming or other disruptive practices, even though this may leave the College computer users unable to communicate with those sites.

While the College takes reasonable measures to protect the security of its computing resources, the College cannot guarantee absolute security and privacy. In cases of administrative or judicial proceedings, information stored electronically may be released

to outside parties. Users should recognize that although access to their files and data is normally avoided, situations may arise where employees with legitimate business purposes may have the need to view information or email or monitor user activity on the network. Causes for access may include, but are not limited to the health or safety of individuals or property; violations of College policies, or local, state or federal laws; termination of an employee; and the need to locate information required for College business.

Program-Specific Policies:
Additional procedures may apply to specific labs and equipment within the College. Consult with the appropriate department to determine availability and proper use.

Pierce College

Computer Labs
The Learning Center offers open access computer use for currently enrolled Pierce students. Our computers are available for class related work only.

Learning Center Policy for Computer, Network,
and Computing Facility Users

Your Privileges and Responsibilities:
Computers, networks, and computing facilities made available by Pierce College for students are the property of Los Angeles Pierce College. These computers, networks and computing facilities are for the completion of academic requirements, scholarship, and college business. Use of the computers and these facilities for academic purposes is a privilege of the students. Use of computers, networks, computing facilities for activities other than academic purposes or college related business is not permitted and disciplinary measures will follow.
PROPER ID IS REQUIRED

ANY VIOLATION OF THE FOLLOWING POLICIES MAY BE GROUNDS FOR EXPULSION FROM THESE FACILITIES:

- Use computers for LAPC class related work only.
- In order to print, pay a printing fee at the Pierce College bookstore; you will need your ID card.
- Due to budget limitations, printing off the Internet is not allowed.
- Copying any copyrighted software is prohibited.
- Installing any programs or files on a computer is prohibited.
- Deleting any programs or files from a computer is prohibited.
- Reconfiguring the hardware or software on the computers in any way is prohibited.
- No food or drinks are allowed in The Learning Center.

- Save your work to your own data disks only.
  - You will be required to log in and log out at the computer station that you use.
  - Observe a one-hour time limit on the computers if others are waiting.
  - Limit breaks from the workstation to 5 minutes if others are waiting.
  - Keep conversations and noise level to a minimum.
  - Turn off your cell phones or put them on silent (calls must be taken outside The Learning Center).
  - Treat equipment and furniture with respect.
  - Students are expected to be respectful of other students at all times, conducting themselves in a manner that does not disturb others.
  - Any form of disruption to other students is prohibited.
  - There is a ten page maximum per print project unless approved by The Learning Center staff.
  - Observe lab hours as posted.

The Learning Center has two computer labs for students to use: TLC 1604, and Bungalow 0398, formerly the Center for Academic Success. Both labs have Microsoft Word 2003 for typing papers for your classes. Students will need to purchase a print card at the student store (minimum $3 purchase) to print documents in TLC 1604 (and TLC 1613). Students wishing to print documents from Bungalow 0398 must bring in their own paper.

Los Angeles Valley College

ELECTRONIC INFORMATION RESOURCES USE POLICY
Adopted Los Angeles Valley College, January 1998, language revised on October 17, 2005

Electronic information resources at Los Angeles Valley College are to be used in a manner that supports the educational mission of the college. The Los Angeles Valley College mission and values encourage teaching and learning, research, creativity, collaboration and the free exchange of ideas in a climate of openness and respect.
Los Angeles Valley College owns, operates and maintains a computer network system including E-Mail, Internet connections, and a website. Specific Web Site Standards, Guidelines, Forms, and Procedures help all users maintain coherence, accuracy, and quality across the college's website. Electronic information resources include, but are not limited to, electronic hardware and software and related communications systems such as e-mail, voice mail, web pages, electronic bulletin boards, fax transmissions and teleconferencing.
In general, the same ethical and professional conduct that applies to other college activities applies to the use of electronic information resources. Users must show respect for college property, the learning environment, and bear responsibility for their actions. The Los Angeles Community College District B-27 defines appropriate ethical and professional conduct for electronic information users. In addition, B-28 define network security policies and procedures. The college's network system is not to be used for private enterprise.

West Los Angeles College

Library Site inaccessible

CSU Dominguez Hills

1. All CLASS facilities and services are for current CSUDH students taking CSUDH courses. Students must show a valid CSUDH Student Identification card to use the center.
2. All students must sign in upon entering and sign out upon exiting.
3. If students want to work with a tutor, they must check in with a student assistant/staff member. Appointments are mandatory for writing tutoring.
4. All CLASS services and facilities are for academic use only.
5. Disruptions to the learning environment will not be tolerated.
6. Cell phone use is NOT allowed in the center.
7. The center is not responsible for lost, stolen or damaged personal property.
8. Students must observe lab hours and abide by the Center Services and Lab Use Policy. Any student who refuses to do so will be suspended from using our services and facilities.
9. Copies of our CLASS Service and Lab Use Policy are posted throughout the center, online and can be requested.

Tutoring Services & Appointments

10. Tutors are learning facilitators who help students develop their academic skills. They will help students review material, find answers to their questions and share learning strategies.
11. Tutors are NOT proofreaders. They will NOT correct assignments, write or type papers, justify grades and complete assignments in any manner.
12. Tutoring sessions are NOT substitutes for missed lectures, readings and research.
13. A Session Log is completed during all formal tutoring sessions. The student is provided a copy of the log for documentation.
14. Tutoring sessions are limited to one 30-minute session in 2 different subjects per day. For example, students may see a Writing tutor and a Math tutor on the same day.
15. Students may schedule only one appointment per day for up to a week in advance. Same day appointments are prohibited.
16. Appointments are cancelled if you are late.
17. Your printed appointment reminder is your documentation for your appointment's date and time.
18. If you miss or cancel 2 consecutive appointments within 7 days, your appointment making privileges will be suspended for a week from the time you schedule your next appointment.
19. We will make every attempt to reschedule appointments if your tutor is unavailable.
20. Students cannot leave papers or assignments.
21. Students must bring their textbooks and course materials to their sessions and attempt to do their work before meeting a tutor.

Writing Tutoring

22. Writing tutoring sessions are limited to one paper per session. Bring a typed/legible draft or prepare questions to ask the tutor.
23. Students must prepare questions or identify specific areas in need of attention if they have a paper longer than 6 pages since sessions are limited to 30-mintues
24. Writing tutors will not proofread or write papers. Instead, they will offer writing improvement and revision strategies.
25. Writing tutors will only work on papers assigned in CSUDH courses. Tutors will not read or provide help with personal memos, resumes, letters, e-mails, websites and fliers.

Math Tutoring

26. Tutors will work with current CSUDH students on CSUDH Math/Science course materials only.
27. Please make sure to attempt to work through all your assigned coursework prior to meeting with a tutor.
28. Math/Science tutors will help you identify patterns of errors and provide correction strategies.
29. Tutors will offer learning strategies, but they are not responsible for completing course assignments, homework, take-home exams and pretests. The student is always responsible for his or her own work.
30. Improvement takes time and effort. It may take more than a few sessions before results can be seen.
31. If you need proof that you have worked with a tutor, please use your copy of the Math/Science Log as proof of your visit.

Computer Use

32. All computer use must be for academic purposes. Online shopping or viewing sites such as Ebay is not permitted.
33. Any file saved on the hard disk will be deleted.
34. No saving or reserving a computer terminal. A computer that has not been in active use for 10 minutes becomes available to the next student who needs a computer.
35. Viewing pornographic inappropriate material or that which creates a hostile work environment will not be permitted.
36. Lab equipment found to be non-functional should be reported to a CLASS staff member.
37. All changes to equipment and software must be made by CLASS authorized personnel.
38. Students must bring or purchase paper for 5 cents a sheet. Bills over $5 will not be accepted, and you may only print 50 sheets per day regardless if you bring or purchase paper.
39. All audio from computers must be heard through headphones. Students may check out headphones at the front desk with a valid CSUDH identification card.
40. No one is permitted access to the network ports.
41. No eating or drinking while using the center's computers.
42. It is the student's responsibility who is downloading or uploading documents to make sure that they are not copyrighted works or that the student has the permission of the

copyright holder.

43. Tutors will assist students only in the following areas: 1) Installing paper in the printer, 2) Navigating the CLASS website, 3) Answering questions concerning access to PLATO, Bedford Handbook & ALEKS, 4) Saving a file on disk. Students may obtain additional help by attending CLASS computer workshops.

Study Rooms

44. Study Rooms are only for studying, tutoring or small group work. Tutoring and small groups have priority over quiet studying. Please yield rooms to tutors and groups if you are using a room alone.

Santa Monica College (SMU) Student Computer Use Policy

The college is providing email and computer access to all students to support your instructional, cultural, and research activities associated with the courses that you are currently enrolled in. By accepting this policy, you agree to the general provisions of all responsible computing policies adopted by the College. Users also agree to follow acceptable use policies established by individual computing labs and network systems and to obey directives issued by authorized College personnel supervising such labs and systems. The activities associated with your computer use need to follow the broad principles established in the Santa Monica College Responsible Computer Use policy. They include carrying out SMC course assignments and activities requiring access to and use of electronic mail and other campus computing facilities and systems. Computing is a privilege to all students at Santa Monica College. As such, you are held accountable for your actions as a condition of continued membership in the College community. By using your account, you acknowledge and agree to abide and conform to the following responsibilities:

SMC computers and networks are to be used primarily for college-related research, instruction, learning, distribution of scholarly information, and administrative activities;

Users shall not attempt to modify any system or network or attempt to crash or hack into college systems. They shall not tamper with any software protections or restrictions placed on computer applications or files. Unless properly authorized, users shall not attempt to access restricted portions of any operating system or security software. Nor shall users attempt to remove existing software or add their own personal software to college computers and systems unless properly authorized;

Users shall use only their own designated computer accounts. Accounts are non-transferable: users shall not use another individual's ID, password or account. Users should respect the privacy and personal rights of others and not access or copy another user's email, data or other files without permission;

Users are responsible for their own computer account(s). They should take precautions against others obtaining access to their use;

Users are responsible for using software and electronic materials in accordance with copyright and licensing restrictions and applicable college policies. Individuals using SMC's computing resources are required to abide by all applicable copyright laws and licenses. Both College policies and the law expressly prohibit the copying of software that has not been placed in the public domain and distributed as "freeware " and use

appropriate precaution to protect their own privacy. "Shareware " users are expected to abide by the requirements of the Shareware agreement. SMC equipment may not be used to violate copyright laws or license agreements. No one may inspect, change, copy or distribute proprietary data, programs, files, disks or software without the proper authority;

Users should remember that information distributed on SMC computers and networks uses college resources and thus represents SMC and not just an individual. Even with appropriate disclaimers, the College is represented by its students, faculty and staff, and so appropriate decorum is warranted;
The College will honor the privacy of individual users, but reserves the right to monitor communications and/or usage when there is just cause, e.g. to remove or compress inappropriate or large files, to investigate user directories and files which may cause or be affected by a system problem;

Due to the open and decentralized design of the Internet and networked computer systems in general, SMC cannot protect individuals against the receipt of material that may be offensive to them Those who use electronic computing on campus are warned that they may receive material that is offensive to them. Likewise, individuals who use email or those who make information about themselves public on the Internet should know that SMC cannot protect them from invasions of privacy.
SMC reserves the right to terminate all accounts and files associated with students who are no longer currently enrolled and taking classes.

Because access to email and computing facilities and systems is a privilege, violation of responsible computer use policies will have consequences. Specifically,
Authorized computer system supervisors may resolve informally unintentional or isolated violations of use policies through email or face-to-face discussion and education with the user or users concerned.

However, repeated violations or misconduct can result in the temporary or permanent loss of computer access privileges or the modification of those privileges. Violations include but are not limited to unauthorized use of computer resources, attempts to steal passwords or data, unauthorized use or copying of licensed software, harassing communication or threatening behavior. Policy violations by students will be handled in accordance with the disciplinary processes described in the Student Code of Conduct

Permissible Use

The Library will monitor usage of library computer workstations to ensure security and operating performance of its systems and networks. Patrons will inform Library staff of equipment problems and are not allowed to tamper with the system.

Students, faculty, and staff with valid Santa Monica College identification cards have priority over other users. The number of Internet access workstations is limited. The Library reserves the right to reclaim workstations being used for personal or recreational

purposes, such as writing letters or surfing the World Wide Web, and to reassign them to patrons who need to identify or access research materials or complete coursework assignments.

Patrons may use computing and networking technologies in the Library with the following restrictions:

A. The use is not for illegal acts under federal or state law, pornography, or gambling.
B. The use does not result in commercial gain or private profit (other than allowable under University intellectual property policies).
C. The use does not violate federal or state laws or College policies on copyright and trademark.
D. If the use is personal or recreational, it does not prevent use by another College community member for legitimate College work.

CHAFFEY COLLEGE COMPUTER AND INTERNET USE

The Library has computers in the Information Research Center with Internet access and Microsoft Office (Word, Excel, Access, Power Point). Use is limited to ***current* students, staff and faculty** and login with Chaffey ID number is required.

Internet access is available for research only. Computer users are expected to abide by Chaffey College Internet Policy.The following activities are not allowed:

- Installing or downloading any software on the hard drives
- Viewing or downloading offensive or obscene materials
- Playing games
- Changing settings
- Viewing music videos
- Instant messaging or chat rooms outside of Blackboard and WebCT

Use of the computers is limited to the software that is already installed. The Reference Desk has a list of the computer labs on campus with their phone numbers, locations, and hours for the semester if there is specific software that you need to use for an assignment

RIO HONDO COMMUNITY COLLEGE INTERNET ACCEPTABLE USE POLICY

Guidelines for Responsible Use of the Internet

The provisions stated in this document serve as an acceptable use policy which governs the use of computers and networks in the Rio Hondo College Library. Please note that the use of computer systems in the Library is a PRIVILEGE, not a right. It is the objective of the Library to maintain an atmosphere of constructive learning, academic freedom, and proper asset management and control. In order to meet this objective, each user is responsible for the use of the computing resources in an effective, efficient, ethical, and lawful manner.

I USER ELIGIBILITY

The Library computers are open-access and available on a first-come, first-served basis to students, staff, faculty, and district residents of Rio Hondo College.

II RIGHTS AND RESPONSIBILITIES

All users must agree to abide by the guidelines established in this Acceptable Use Policy Each user must understand and acknowledge that his/her freedom to access and display information is constrained by the rights of others.

No person may use Library computer resources for any illegal or unauthorized act. Specifically, individuals may not use computing resources to violate any state or federal laws or any regulation of Rio Hondo Community College including, but not limited to, any laws and regulations governing the creation, dissemination, or possession of pornography or other illegal documents or images; the possession or use of programs, files or instructions for violating system security; and the violation of copyright law. Library computer resources may not be used to intimidate or create an atmosphere of harassment based upon gender, race, religion, ethnic origin, creed, or sexual orientation. Fraudulent, threatening, or obscene email, graphics, or other electronic communications are prohibited.

Changing, modifying, or eliminating Library computer configurations and loading any application or program software onto the Library computers is prohibited.

The availability of Internet resources will be determined by staff at Rio Hondo College Library. As of this writing, non-course-related chat or chat-like activities are NOT allowed.

III POLICY VIOLATIONS

If a computer user violates any of the acceptable use provisions outlined in this document, his/her computer privileges will be terminated and future access may be denied. Some violations constitute a criminal offense and may result in legal action and/or other penalties as deemed warranted by the Vice President for Student & Academic Services.

IV AGREEMENT
Note: Using the Library Internet computers constitutes acceptance of this agreement.
I understand that to use the Library Internet computers, I must be a currently registered borrower in good standing of the Rio Hondo College Library.
I understand that the use of the Internet computers is a privilege, not a right, which may be revoked at any time for inappropriate conduct.
I agree to report any hardware or software malfunctions to the Library staff immediately.
I understand that the Rio Hondo College Library is not responsible for any damage to computer diskettes, or personal computer equipment.
I understand that the Internet computers are in a public environment and accept that privacy is not guaranteed.
I understand that I may not use non course-related chat or chat-like activities on the Library Internet computers.
I understand that any failure on my part to comply with the stipulations of this Agreement and the Library's Acceptable Use Policy: Guidelines for Responsible Use of the Internet may result in the suspension of my Library Internet privileges and possible disciplinary action.
I acknowledge that I have read "Guidelines for Responsible Use of the Internet" and this Agreement and I agree to follow the Acceptable Use Policy.

Humboldt State University

Planning: Appropriate Use Policy

Overview
This document borrows extensively from and replicates significant portions of the University of Delaware's "Policy for Responsible Computing." The University of Delaware was awarded CAUSE's "Best Practices in Service" award for 1995 for this work. Local modifications and editing were performed by a committee of users in 1996, including faculty, staff, and students, appointed by the Vice President for Academic Affairs. Some wording in the document was updated in 2001 to bring the wording into conformance with the **California State University 4CNet** Appropriate Use Policy (2000) and its Recommended Contextual Standards for Appropriate Use Policies (2000).

Preface
It is imperative that all users of the College’s computing, communications, and information resources realize how much these resources require responsible behavior from all users. Simply put, we are all responsible for the well-being of the computing, network, and information resources we use. Colleges do try to promote the open exchange of ideas; however, an open, cooperative computing network can be vulnerable to abuse or misuse. As more and more schools, colleges, universities, businesses, government agencies, and other enterprises become attached to the world-wide computing and information networks, it is more important than ever that this College educate its students, faculty, and staff about proper ethical behavior, acceptable computing practices, and copyright and licensing issues. A modern college must also

educate its students, faculty, and staff about how computer abuse can interfere with the exchange of ideas that is integral to a modern education. The first item in the body of this document is the Policy for Responsible Computing at the Humboldt State University, approved by the Executive Committee of Humboldt State University on September 19, 1996. The remainder of this document consists of guidelines for implementing this policy.

In support of its mission of teaching, research, and public service, Humboldt State College provides access to computing, communications, and information resources for students, faculty, and staff within institutional priorities and financial capabilities. The Humboldt State Appropriate Use Policy contains the governing philosophy for regulating faculty, student, and staff use of the College's computing, communications, and information resources. It spells out the general principles regarding appropriate use of data, equipment, software, and networks. By adopting this policy, the Executive Committee recognizes that all members of the College are also bound by local, state, and federal laws and other statutes relating to copyrights, security, electronic media and intellectual property.

The Policy
All users of the College's computing, communications, and information resources must act responsibly. Every user is responsible for the integrity of these resources. All users of College-owned or College-leased computing and communications systems, whether managed directly or indirectly by the campus, must respect the rights of other computing and communications users, respect the integrity of the physical facilities and controls, and respect all pertinent license and contractual agreements. It is the policy of Humboldt State College that all members of its community act in accordance with these responsibilities, relevant laws and contractual obligations, and the relevant faculty, staff and student standard of ethics and conduct. Additionally, all users must comply with the California State University CENIC Appropriate Use Policy.

The College reserves the right to limit, restrict, or extend computing privileges and access to its information resources. Access to the College's computing and communications facilities is a privilege granted to Humboldt students, faculty, and staff. Access to Humboldt information resources may be granted by the data owners based on the data owner's judgment, which would include the following factors: relevant laws and contractual obligations, the requestor's need to know, the information's sensitivity, and the risk of damage to or loss by the College.

Data owners--whether departments, units, faculty, students, or staff--may allow individuals other than University faculty, staff, and students access to information for which they are responsible through methods approved by and at the discretion of the system administrator, so long as such access does not violate any license or contractual agreement; University policy; or any federal, state, county, or local law or ordinance; or degrade the performance of the University's information service to the detriment of the University community.

University computing and communications facilities and accounts are to be used for the University-related activities for which they are assigned. All computing and network resources are provided only to support the academic mission of the University. University computing and communications resources are not to be used for commercial purposes or non-University-related activities without written authorization from the University. If the University grants such authorization, the University may assess appropriate charges to recover the costs of providing such services. This policy applies equally to all University-owned or University-leased computers and network resources.
Abuse of computing and/or communications privileges is subject to disciplinary action as well as loss of computing and communications privileges and/or the assessment of fines to recover any costs for investigations and the value of resources used. Abuse of the University's computing and communications resources may also result in loss of university privileges, dismissal, or civil/criminal action. Nothing in these guidelines precludes enforcement under the laws and regulations of the State of California, any municipality or county therein, and/or the United States of America. For example, if a user is found guilty of committing a computer crime as outlined in the California Penal Code 502, Computer Crimes, and 502.1, Computer crime penalty, forfeiture of property, he or she could be subject to the penalties for a felony.

- Using computing facilities, computer accounts, or computer data for purposes other than those for which they were intended or authorized.
- Sending fraudulent computer mail, breaking into another user's electronic mailbox, or reading someone else's electronic mail without his or her permission.
- Sending any fraudulent electronic transmission, including but not limited to fraudulent requests for confidential information, fraudulent submission of electronic purchase requisitions or journal vouchers, and fraudulent electronic authorization of purchase requisitions or journal vouchers.
- Violating any software license agreement or copyright, including copying or redistributing copyrighted computer software, data, or reports without proper, recorded authorization.
- Violating the property rights of copyright holders who are in possession of computer-generated data, reports, or software.

Using the College’s computing resources to harass or threaten other users. Harassment includes, but is not limited to, any behavior that involves an expressed or implied threat to an individual's academic efforts, employment, participation in College-sponsored extracurricular activities or personal safety; OR has the purpose or reasonably foreseeable effect of interfering with an individual's academic efforts, employment, participation in College-sponsored extracurricular activities or personal safety; OR creates an intimidating, hostile or demeaning environment for educational pursuits, employment or participation in Colleges-sponsored extracurricular activities

- Taking advantage of another user's naivete or oversights to gain access to any computer account, data, software, or file that is not your own and for which you have not received explicit authorization to access.
- Physically interfering with other users' access to the College’s computing facilities.

- Encroaching on others' use of the College’s computers (e.g., disrupting others' computer use by excessive game playing; by sending excessive messages, either locally or off-campus, including but not limited to electronic chain letters; printing excessive copies of documents, files, data, or programs).
- Modifying system facilities, operating systems, or disk partitions; attempting to crash or tie up a University computer; damaging or vandalizing University computing facilities, equipment, software, or computer files.
- Disclosing or removing proprietary information, software, printed output or magnetic media without the explicit permission of the owner except when so authorized as a system administrator or performing the duties of supervisor.
- Reading other users' data, information, files, or programs on a display screen, as printed output, or via electronic means, without the owner's explicit permission except when so authorized as a system administrator or performing the duties of supervisor.
- Using university facilities for commercial use or profit unless specific contractual agreements have been made.

Administrative Process for Cases of Misuse of Computing, Communications, or Information Resource Privileges

If staff or system administrators have information that intentional or malicious misuse of computing resources has occurred, and if that evidence points to the computing activities or the computer files of an individual, they have the obligation to pursue any or all of the following steps to protect the user community:

- Take action to protect the system(s), user jobs, and user files from damage.
- Notify the alleged abuser's project director, instructor, academic advisor, dean, or administrative officer of the investigation.
- Refer the matter for processing through the appropriate College administrative process. If necessary, staff members from a central computing agency such as Information Technology Services as well as faculty members with computing expertise may be called upon to advise the College University judicial officers on the implications of the evidence presented and, in the event of a finding of guilt, of the seriousness of the offense.
- Suspend or restrict the alleged abuser's computing privileges during the investigation and administrative processing. A user may appeal such a suspension or restriction and petition for reinstatement of computing privileges through the College’s administrative system, through the grievance procedures outlined in the HUMBOLDT College Catalog, as appropriate.
- Inspect the alleged abuser's files, diskettes, and/or tapes. System administrators shall have a trail of evidence that leads to the user's computing activities or computing files before inspecting any user's files. (See "System Integrity" of these Guidelines for more information.) Ordinarily, the administrative officer whose department is responsible for the computing system on which the alleged misuse occurred should initiate the administrative proceedings. As the case develops, other administrative officers may, by mutual agreement, assume part of the responsibility for prosecuting the case.

- Ordinarily, the administrative officer whose department is responsible for the computing system on which the alleged misuse occurred should initiate the administrative proceedings. As the case develops, other administrative officers may, by mutual agreement, assume part of the responsibility for prosecuting the case.

Academic Honesty

Students are reminded that computer-assisted plagiarism is still plagiarism. Unless specifically authorized by a class instructor, all of the following uses of a computer are violations of the Colleges guidelines for academic honesty and are punishable as acts of plagiarism:

- copying a computer file that contains another student's assignment and submitting it as your own work.
- copying a computer file that contains another student's assignment and using it as a model for your own assignment.
- working together on an assignment, sharing the computer files or programs involved, and then submitting individual copies of the assignment as your own individual work.
- knowingly allowing another student to copy or use one of your computer files and to submit that file, or a modification thereof, as his or her individual work.

Appropriate and Inappropriate Use

1. It is impossible to provide an exhaustive definition of inappropriate computer use, or a complete set of examples to cover every conceivable situation. Users who have questions about which computer uses are appropriate and which are not should inquire about their intended use by contacting the IT department. Without limitation, the following examples shall be construed by all of the campus community as examples of inappropriate use of technology resources:

- users shall not interfere with system performance or another user’s use of the system
- users shall not disclose their passwords or lend their account to any other individual, apart from IT staff
- users shall not gain access to accounts, files, passwords or resources intentionally and
- without authorization of the account holder
- users shall not use technology resources for non-District fundraising or commercial
- purposes.
- users shall not use technology resources for any activities which violate state or federal laws.

Computing resources may not be used to intimidate, threaten or harass individuals, or violate the college's policies concerning relationships between college constituencies. Such activities include, but are not limited to, using computing resources to store, print, or send obscene, slanderous, or threatening messages.

2. Users may use their computers and network accounts for non-District matters except as

otherwise prohibited by this or other District policy or where such use unreasonably interferes with academic uses, job performance or system performance/operations. Such use is subject to the terms of this policy including, without limitation, terms regarding access to information on District computers and accounts.

a. Any and all information maintained on District-owned computers/network accounts, whether District-related or not, is accessible by the District. Other than to perform routine operations or as may be legally required, the District will not monitor accounts or access the information stored in computers/network accounts without the user's consent unless such action is necessary to enforce this policy.

b. Employees are strongly encouraged to remove any "personal" information they may have stored on their computers/network accounts prior to ending their relationship with the District. The District may destroy information left on computers/network accounts. Information will be retained if retention is in the District's best interest. If the District extends an individual's account access beyond the employment separation date, the account is not subject to this provision until the extension has ended.

Process for Suspension and Termination of Use

Users understand that violation of this regulation may result in suspension or termination of computer, network account and other access and, depending upon the circumstances, may result in disciplinary action. Violations will be processed through normal District channels. If the activity is also unlawful, it may result in criminal and/or civil prosecution.

1. Emergency Suspensions

a. In the event of a perceived emergency or where other exigent circumstances demand immediate action, the Vice President responsible for Information Technology or designee may immediately suspend computing privileges and notice will be given to the user as soon as reasonably possible.

b. The District may temporarily suspend a user's computing privileges for security or other administrative reasons. Computing privileges suspended pursuant to this provision will be restored as soon as the threat or concern has been addressed or within three business days, whichever is shorter. Accounts that are suspended for more than three days will be handled as outlined below, irrespective of whether disciplinary action has been initiated. Absent extenuating circumstances, no account may be suspended pursuant to this policy for more than 10 business days, unless the disciplinary process has been invoked.

2. Non-Emergency Suspensions and Terminations

a. In non-emergency situations, the Vice President responsible for Information Technology or designee will provide the user with notice of the perceived problem and an opportunity to be heard before privileges are suspended.

b. A suspension may be appealed in writing to the Vice President of Human Resources or designee within three business days of the effective date of the suspension. The Vice President of Human Resources or designee will provide a written decision to the Vice President responsible for Information Technology and the user within five business days of receipt of the appeal. The Vice President of Human Resources' or designee's decision will remain in effect pending final resolution of the disciplinary proceeding.

c. Suspected violations by District employees will be reported to the employee's supervisor and handled through established channels for disciplinary action.
d. Pending resolution of the disciplinary process, the Vice President responsible for Information Technology or designee may suspend District computing privileges if the alleged violation is reasonably perceived to constitute unlawful activity, pose a substantial risk to the integrity of campus computing or present an imminent threat to the safety or welfare of the campus or members of the college community.
e. Sanctions for violations of this regulation will be imposed by the administrative official with final responsibility for resolution of the disciplinary process in use, following consultation with the Vice President responsible for Information Technology in the event that sanctions involve campus computing services. Sanctions with respect to campus computing services may include, but are not limited to, suspension or permanent revocation of computing privileges. The District reserves the right to seek restitution and/or indemnification from an employee for damages arising from violations of this regulation. In addition, the District and/or third parties may pursue criminal and/or civil prosecution for violations of law.
f. A suspension may be appealed in writing to the Vice President of Human Resources or designee within three business days of the effective date of the suspension. The Vice President of Human Resources or designee will provide a written decision to the Vice President responsible for Information Technology and the user within five business days of receipt of the appeal. The Vice President of Human Resources' or designee's decision will remain in effect pending final resolution of the disciplinary proceeding.
Personal Responsibility
1. As a representative of the District, users must accept personal responsibility for reporting any misuse of the network to relevant IT staff. This includes, but is not limited to, users who suspect that their District-provided computers or network accounts have been accessed without their permission. These users are expected to change their password as soon as it is reasonably possible to do so and to report the suspected activity to relevant IT staff.
2. Users are responsible for all use of computers and network accounts provided to them by the District, including backup of files on their district-provided computer and password maintenance.
a. Responsible use includes using passwords that are not easily deduced by others.
b. Voluntary unauthorized disclosure of a password may result in suspension, revocation and/or denial of computing privileges. Disclosure of passwords to Information Technology (IT) staff or other District system administrators is considered authorized disclosure.
c. District-provided network accounts may only be used by the user to whom they are assigned unless otherwise authorized by the District. Access to computers and network accounts for maintenance/service purposes by persons responsible for systems and IT is considered authorized; users are not responsible for actions taken by these persons.
d. Users who suspect that their District-provided computers or network accounts have been accessed without their permission are responsible for changing their passwords and are strongly encouraged to report the suspected activity to IT.
e. Users are responsible for actions for others who use their network accounts with their permission.

f. Users are responsible for logging off and for protecting their private account.
g. Users need to be responsible for choosing passwords that are not easily guessed by others.

On a regular basis and in accordance with the current security practices of the computing industry, IT staff may require users to change their passwords. The voluntary, and unauthorized disclosure of a user password may result in the suspension, revocation and/or denial of computing privileges in the future.
Users gain access to computer systems by being assigned an account on the college's computer network.

Possession of an account may allow its owner to access various systems, databases, student records, websites and use peripheral devices such as printers. Each employee member is assigned an account for his/her use in their professional activities.

Colorado School of Mines (CMS**)** Computing & Networking Resource and Responsible Use Policies & Guidelines Related policies, agreements, processes, and guidelines AC&N System & Network Administrator Policies

I. PURPOSE

This policy has been established to provide guidelines for the acceptable and responsible use of computing and networking resources provided for use by Colorado School of Mines employees, students, and other users in order to set forth the expectations and responsibilities of those who use the resources. Procedures used when violations of these and related policies occur are addressed in the document titled “Investigation of and Response to Policy Violations”, also referred to as AC&N Policy Violations Processes.

II. POLICY

A. Introduction

Computing and networking resources made available to current students, faculty, staff and other users at Colorado School of Mines are to be used in a manner consistent with the instructional, research and administrative objectives of the Colorado School of Mines. The ethical and legal use of any computing and networking resource is the responsibility of each resource user.

B. Policy Development Principles and Guidelines

The following principles govern the development and implementation of CSM computing and networking (also known as information technology) related resource policies:

1. Usage policies should protect and be in the best interest of the CSM community of users.
2. Free inquiry and expression are essential elements of the academic enterprise. Usage policies should not infringe the academic freedom or rights to free speech of community members.
3. CSM computer systems, networks, and related resources are provided primarily for the academic and CSM business use of currently enrolled students and current faculty and staff of CSM.
4. CSM is a state institution and is subject to State of Colorado statutes, policies, or executive orders that involve the use of State resources. Computing and Networking

resource users are expected to comply with all State requirements.
5. CSM community users should have fair and equitable access to shared resources.
6. Computing and Networking resource users are expected to be responsible electronic citizens.
7. Reasonable amounts of central computer system and network resources are provided at no direct or metered usage charge to faculty, staff and students to accomplish tasks relating primarily to classroom instruction and preparation, administration and related scholarly activity, and appropriate research or special projects sanctioned by the School.
8. Electronic communication is a common form of personal interaction in today's world and access to computing and networking resources is an important element in a student's college experience and the life of any educated person.
9. CSM computer systems, data, networks, and related resources are valuable assets whose integrity must be maintained. Such integrity is partly maintained through the effective management, security, and protection of the resources used.
10. It is recognized that computing or networking resources may be a medium used in violating other institutional policies.
11. CSM accommodates and does not interfere with standard technical measures, as defined in Title 17, Chapter 5, Section 512(i)(2) of the United States Code.

C. Responsibilities and Acknowledgements

Any individual who accesses CSM-administered computing and networking resources
1. is expected to use all resources in a responsible and ethical manner;
2. is required to exercise reasonable means to protect campus resources from abuse or misuse;
3. is responsible for all activity that occurs under any account that is assigned or registered to them or from a computer or other device that is owned by the institution and provided for their use (such as an office computer);
4. is responsible for all activity that occurs on an institutionally-owned portable, laptop, or other computer or network-attached device that is loaned to them while the device or computer is in their possession;
5. is responsible for all network activity that occurs from a personally-owned computer or other device which they have connected to the campus wired or wireless network;
6. must use reasonable means to protect data, account passwords, and access to the campus network through their computer or other network-attached device. This includes the responsibility to create good passwords and keep them private, update personally-owned or administered computers and applications with security patches, and preventing systems and applications from damaging or harassing others on or off campus via any network.
7. should be familiar with and comply with applicable laws, licensing requirements, CSM policies, guidelines, and generally accepted usage practices.
8. accepts that network and system administrators may examine electronic files and network transactions to adequately manage resources. Administrators are expected to treat the contents of such files and traffic as private and confidential. Inspection of content, and action as a result of such inspection, will be governed by applicable School policies, Colorado and U.S. law.

9. is permitted limited personal use of computing and networking resources so long as such use
    a. complies with all state and federal law and campus policies,
    b. does not create resource or management problems,
    c. does not interfere with or disrupt academic and other legitimate use,
    d. does not interfere with their professional obligations and duties to CSM,
    e. does not interfere with the professional responsibilities or activities of other CSM community members, and
    f. is not used to support any activity or provide any service for which the user receives any type of compensation other than from CSM. Academic and campus administrative use of all resources supersedes personal uses in all instances, however.
10. acknowledges that disciplinary actions administered due to violations of other CSM policies may include temporary or permanent suspension of computing and networking access in appropriate situations.

D. Prohibited Activities

Engaging in activities such as those listed below is prohibited by this policy and in some cases other institutional policies. Violations may result in temporary or permanent account suspension, disciplinary action, or legal action if appropriate. In addition to the sanctions or disciplinary actions defined in other CSM policies, the suspension or revocation of access to some or all computing resources, and/or suspension or termination of network connections are possible sanctions that can be imposed by the appropriate administrative authority. Examples of prohibited activities include, but are not be limited to:

1. electronic cheating and plagiarism in any form
2. undermining, or attempting to undermine, the security, integrity, or operations of computing systems or network resources, on or off campus
3. exploiting security weaknesses or bugs in computer systems or network devices connected to the campus or any external network
4. probing on- or off-campus systems or networks to expose security or access weaknesses
5. intentional attempts to deny service or create problems with the operation of computer systems or the network
6. using campus resources as a staging ground or pathway to attack or exploit weaknesses in computer systems on or off campus
7. using campus resources to commit any criminal or illegal act, or violate any CSM policy
8. sharing your EKey, PINs and/or password or allowing others (on or off campus) to use your accounts or network access
9. using any CSM computer account that is not yours with or without permission of the account owner. In specific situations, faculty and staff can delegate authority to access their account only to another CSM employee and only with proper written notification to the resource manager.
10. using any CSM computer or network resource without proper authorization.
11. accessing the email, files, data, and other resources on or off campus that are not yours without the permission of the resource owner

12. installing network service devices such as hubs, switches, routers, and wireless access points and services without express written permission from AC&N
13. installing software or files requiring a license on any campus computer without proper authorization
14. installing software on computer laboratory systems without permission from the lab system administrator
15. distributing from any network-attached device software or files requiring a license without proper authorization
16. infringing on any copyright, trademark, or patent
17. using campus-owned computers or network access to support any activity or provide any service for which the user or anyone else receives financial compensation other than from CSM.
18. sending unsolicited mass e-mail (spam) or chain letters on or off campus
19. knowingly spreading electronic viruses, worms, or trojan horses through e-mail or any other method
20. using e-mail or any computer or network resource to harass any individual or group of people
21. representing yourself as someone other than yourself in any e-mail or other form of Electronic communication sent to CSM faculty, staff, or other students
22. deliberately damaging or physically abusing any computing or network resource
23. offering any services (such as DHCP, DNS, or others) that may disrupt or interfere with enterprise-wide services provided by AC&N or Information Services
24. offering any services or information, via CSM's network or through accounts on CSM computers, without permitting inspection of the services or information by authorized CSM computing support personnel
25. consuming shared resources (such as cpu time, disk space, and network bandwidth) to the extent that others cannot access the resources or disrupting the ability of others to effectively use shared resources

E. Policy Violations

Investigation of policy violations and the potential consequences or actions taken as a result of an investigation or infraction are outlined in the document titled “Investigation of and Response to Policy Violations”. This document is also referred to as the AC&N Policy Violations Processes document. For detailed information, see http://www.mines.edu/academic/computer/policies/PolicyViolationsProcesses.pdf

III. REMINDERS & RECOMMENDATIONS

A. Please remember...

1. that EKeys and passwords should never be shared with anyone. Support staff members do not need that information to assist you with a problem. When working in public labs, do not leave your computer unattended for long periods of time. If you leave it even for a short period of time (a few minutes), you are still responsible for any activity that occurs under your account. When finished or leaving for an extended period of time, be sure to log out.
2. that personal home pages must provide an obvious link from their top level home page to the disclaimer located at http://www.mines.edu/students/Disclaimer.shtml
3. to become familiar with all policies and guidelines relating to the use of computing and Networking resources. Links to related policies, agreements, and guidelines are listed

at the beginning of this document.

4. to not display materials that could be considered offensive by the application of reasonable standards on computers in shared work areas such as computer labs and the Library.
5. to be careful with equipment and considerate of others by using good judgment and cleaning up thoroughly when you are finished in a work area. Light snacks and soft drinks may be acceptable in some labs but pizza and other messy foods, as well as alcoholic beverages are forbidden. If you spill something, clean it up, and please return chairs to their proper location.
6. that although it is the responsibility of each department head to manage the use of computer resources operated by his or her department, the policies established by departments to govern the use of local computer resources cannot conflict with the above policies and are subject to approval by the appropriate administrative authority within CSM.
7. that CSM subscribes to the spirit of the EDUCAUSE code regarding intellectual property and the legal and ethical use of software: Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to works of all authors and publishers in all media. It encompasses respect for the right to acknowledgement, right to privacy, and right to determine the form, manner, and terms of publication and distribution. Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environments.

Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorized access, and trade secret and copyright violations, may be grounds for sanctions against members of the academic community.

B. We recommend that you...

1. learn about and implement security on any system you own and connect to the campus network or any other network (see our Getting Started pages for links to security information);
2. employ appropriate security measures on any system you use;
3. install virus protection software on your computer and update it regularly (learn more here!);
4. backup your system and important data files on a regular basis;
5. install anti-spyware software on your computer and keep it updated;
6. install firewall software on your computer and update it regularly;
7. be wary of executable programs and application files (word processing, spreadsheet, etc.) sent to you as email attachments. Open executable attachments only if they come from a trusted source and check them with virus protection software;
8. learn how to view and read the basics of e-mail headers, sometimes referred to as “full headers”;
9. do not run a program unless you trust the source and are fully aware of what the program will do;
10. do not download files over the Internet unless you trust the source
11. learn more about computer ethics through our ethics links and other sources

Ethics and Information Technology
http://www.mines.edu/academic/computer/ethics/

The following links have been created as a starting point to help members of the CSM community learn more about CSM policies as well as the ethical issues associated with the use of information and communications technologies in our society. Please send comments, or suggestions for additional links to webmaster@mines.edu

CSM Information
- Resource Policies & Guidelines
- Campus E-Mail Policy
- Digital Millenium Copyright Info
- Personal Home Page Policy
- CC Lab Reservation & Use
- CC PC Software Install Policy
- Creating a Good Password

Netiquette
- FAU User Guidelines,Netiquette
- Netiquette Index from PBS

Ethics in Computing Links
- Ethics in Computing (NC State)
- Computer Ethics - Cyberethics
- Interactive Comp Ethics Explorer
- Ethics on the Internet (article)

Cyberspace Law for Non-Lawyers

Security
- SANS
- Security Links from NIH
- W3C Security Resources
- Symantec Anti Virus Res Ctr

Identity Theft
- FTC ID Theft Information
- Dept of Justice Information
- Privacy Rights Clearinghouse

Brint Intellectual Property Links

Copyright
- United States Copyright Office
- Copyright & Fair Use (Stanford)
- Assoc. of Research Libraries
- The Copyright Website

Copyright & Music on the Internet
- Soundbyting (RIAA)

Trademark & Patents
- U.S. Patent & Trademark Office
- PTC World
- Intellectual Property Law Server

Software Licensing & Piracy
- What is Software Piracy?
- SPA Anti-Piracy Initiative
- Chronicle: Students Arrested
- CNN Story: SW Licensing Law
- Warez Myth vs. Fact
- Anti-Piracy Press Releases

Spamming & Chain Letters
- Sample Policies
- CAUCE
- Chain Letter Info from Rutgers
- CIAC Info on Chain Letters

Free Speech, Privacy, Anonymity
- Electronic Privacy Info Center
- Electronic Frontier Foundation

Santa Barbara City College- Santa Barbara City College
Policies For Student Use Of Computers And Networks

Use of college computers by students and access by students to college computer networks and to the Internet are services made available to students to further the educational mission of the College. In order to be granted these access privileges and to retain them, students must abide by the policies and guidelines described in this document.

Computers and networks can provide access to resources on and off campus, as well as the ability to communicate with other users worldwide. Such open access is a privilege, and requires that individual users act responsibly. Users must respect the rights of other users, respect the integrity of the systems and related physical resources, and observe all relevant laws, regulations, and contractual obligations.

Appropriate use
The College provides students with access to computers and computer networks for educational purposes. Use of college computers or networks for other purposes is not permitted. This prohibition includes, but is not limited to, exchanging electronic mail and accessing materials or information on the network if not relevant to the instructional or related functions of the College.

Students are required to adhere to the posted usage policies of student labs or facilities they wish to use. These policies will be posted in or near the facility, and relate to such things as which students are allowed to use the facility, time limits, reserved hours of usage, restricted activities, etc.

Game playing using college computers is not allowed, with the exception of educational games that have been assigned as part of a college course or certain games authorized for use in one or more student labs because they are considered to have an academic purpose. Note that some labs do not allow any game playing at all.

It is prohibited to use college computers for any activity that is commercial in nature, i.e. paid for by non-college funds. Commercial activities include, but are not limited to, consulting, typing services, and developing software for sale. Exceptions to this prohibition are certain internships and work experience programs when specifically approved in writing by the appropriate college authority.

Security and passwords
The security of computer systems is based to a great extent on passwords. Therefore it is important to take your password very seriously, and to keep it secret at all times. Do not select an obvious password, and change your password any time there is any chance that someone else may have learned it. Your password is for your protection. It ensures that no one can make unauthorized use of your computer account. Use of any other user's

account or loaning the use of your account is prohibited. Do not attempt to capture or use any other person's password or account, even for fun or as a joke.
Note that educational networks intrinsically are not secure. Normally student files and electronic mail are private, but this cannot be guaranteed.
Software copying
With only a few exceptions, software on college computers and networks is licensed for use on college computers only. Copying software from a college computer or network is prohibited unless specifically authorized in writing by an appropriate college authority. Illegal copying of software is subject to civil damages and criminal penalties including fines and imprisonment.

Examples of Misuse
Examples of misuse include, but are not limited to, the activities in the following list.
o Using a computer account that you are not authorized to use, attempting to monitor or tamper with another user's electronic communications, or reading, copying, changing, or deleting another user's files or software without the explicit agreement of the owner. Files owned by individual users are to be considered private property, whether or not they are accessible by other users.
o Obtaining a password for a computer account without the consent of the account owner. If you as an authorized user give out your account and password to another individual, you can still be held accountable for any actions that may arise that are associated with your account.
o Using the Campus Network to gain unauthorized access to any computer systems, or attempting to circumvent data protection schemes or uncover security loopholes. This includes creating and/or running programs that are designed to identify security loopholes and/or decrypt intentionally secure data. This also includes programs contained within an account, or under the ownership of an account that are designed or associated with security cracking.
o Knowingly or carelessly running or installing on any computer system or network, or giving to another user, a program intended to damage or to place excessive load on a computer system or network. This includes, but is not limited to, programs known as computer viruses, Trojan Horses, and worms.
o Violating terms of applicable software licensing agreements or copyright laws.
o Deliberately wasting/overloading computing resources, or in any other way knowingly or carelessly performing an act which will interfere with the normal operation of computers, terminals, peripherals, or networks. This includes, but is not limited to, printing multiple copies of a document or printing out large documents that may be available on-line, or that might impact significantly on other users printing resources.
o Using electronic mail to harass others, including sending electronic mail that the sender would reasonably anticipate to be unwelcome.
o Creating mail or electronic distribution lists larger than 10 addressees that send electronic communications to other accounts without prior permission of the receiving individual.
o Moving large files across networks during peak usage periods or prime hours such that it degrades resource performance. Prime hours will be considered to be Monday through Friday from 8:00 am to 5:00 pm.

o Masking the identity of an account or machine. This includes, but is not limited to, sending mail anonymously.
o Posting on electronic bulletin boards or any type of electronic forum information that may be slanderous or defamatory in nature or any materials that violate existing laws or the college Standards of Student Conduct.
o Displaying sexually explicit, graphically disturbing, or sexually harassing images or text in a public computer facility, or location that can potentially be in view of other individuals.
Activities will not be considered misuse when authorized in writing by appropriate college authorities for security or performance testing.

Enforcement
Penalties may be imposed under one or more of the following: SBCC Standards of Student Conduct, California law, the laws of the United States. All existing laws (federal and state) and the regulations listed in the SBCC Standards of Student Conduct document apply, including not only those laws and regulations that are specific to computers and networks, but also those that may apply generally to personal conduct.
Minor infractions of this policy, when likely accidental in nature, such as poorly chosen passwords, overloading systems, excessive disk space consumption, and so on are typically handled in an informal manner by electronic mail or in-person discussions.
More serious infractions are handled via formal procedures:
Infractions such as sharing accounts or passwords, harassment, or repeated minor infractions as described in, but not limited to, the above policies may result in the temporary or permanent loss or modification of computer access privileges, and notification of the Dean of Student Services. Warning! Loss of the privilege of using college computers, even if temporary, may prevent a student from completing course assignments and from making normal progress in the course. This is very likely to have a negative impact on the final course grade.
Offenses which are in violation of local, state or federal laws will result in the immediate loss of all computing privileges, and will be reported to the appropriate college and law enforcement authorities.

Legal Context
Student files are considered "educational records" as covered by the Family Educational Rights and Privacy Act of 1974 (Title 20, Section 1232(g) of the United States Code). Such records are considered confidential under the law, but student files and electronic mail may be subject to search under court order if such files are suspected of containing information that could be used as evidence in a court of law. In addition, system administrators may monitor network traffic and/or access student files or electronic mail as required to protect the integrity of computer systems (e.g., examining files or accounts that are suspected of unauthorized use or misuse, or that have been corrupted or damaged).

Misuse can be prosecuted under applicable statutes. Students may be held accountable for their conduct under any applicable college policies. Complaints alleging misuse will be directed to those responsible for taking appropriate disciplinary action as specified under "Enforcement."
Illegal copying of software protected by United States Copyright Law is subject to civil damages and criminal penalties including fines and imprisonment.
Other organizations operating computing and network facilities that are reachable via the Internet may have their own policies governing the use of those resources. When accessing remote resources, students are responsible for obeying both the policies set forth in this document and the policies of the other organizations.

Disclaimer
College staff responsible for the computer technology will make every effort to ensure the integrity of the computer systems and of the information stored on them. However, students must understand that the College does not take responsibility for the safe storage of student files. Students must keep their own copies of any information that is important to them. Santa Barbara City College is not responsible for any loss of information from college computers or networks, regardless of the cause.
Information posted by students on computer bulletin boards, electronic forums, Web pages, or other publicly accessible sites administered by the College, is subject to review for conformity with legal requirements, including copyright provisions, and with the computer policies described in this document. Postings found to be unacceptable will be removed.

In order to keep the computer labs running as an effective learning environment and to promote a spirit of mutual courtesy and respect, the CLRC has rules that must be followed.

****Violation of These Rules May Lead to Revocation of Lab Privileges, Disciplinary Action from SBCC or other legal actions****

Students using the labs must comply with the SBCC Electronic Communications Policies
and
SBCC Student Use Policy of Computers and Networks.

- Every student, faculty and staff member must **check in at the LAC counter** to use CLRC resources.
- To check-in to a CLRC resource, a student must show his or her own **valid SBCC photo ID** and must be enrolled in the current semester. Faculty and staff must show an SBCC ID.
- **Seating** at the computers in the lab is limited. To prevent overcrowding and to keep a quiet environment for students who are working on assignments, students who are not checked-in will be asked to leave the lab.
- Students who need to work in **groups** may sign up for open hours in CAI_1. The sign-up sheet can be found at the LAC counter.

- Students are required to **check out** of their workstation when they leave. Allowing someone else to use your ID to check in or use a computer you have checked into is a violation of lab rules.
- Work on the computer must be related to **assigned** class work. Students using the computer for **non-academic** purposes will be asked to leave.
- **Game playing** using CLRC computers is not allowed.
- **Printing** of Internet documents is NOT allowed. Printing from the Internet may be done in the Library for a fee. For more details please review our **Printing Policy**
- Students **may print** only one draft and one revised final copy of academic assignments. Printing of non-academic documents is not allowed. Print Preview should be used as much as possible to proofread documents on the screen before they are printed. Extra copies can be purchased in the library.
- The absolute **safety of files** stored on the network drive cannot be guaranteed. Students are responsible for keeping critical files on their own disks.
- Report **computer problems** to a tutor; do not attempt to fix them yourself.

Students are expected to conduct themselves in accordance with SBCC Standards of Student Conduct.

- **Disruptive behavior**, such as shouting or cursing will not be tolerated.
- **Rude behavior** towards CLRC staff will not be tolerated.
- The lab is a quiet area. **Talking** should be minimal.
- Please turn **cell phones** and pagers off or put in inaudible mode. Take all cell phone conversations outside.
- Appropriate **attire** is required in the labs.
- Students should leave workspaces **clean** - chair pushed in, garbage thrown away, etc.
- Please **recycle** paper by placing it in the recycle baskets.
- **No Food or drink** (including water) is allowed as they can damage computer equipment.
- **No children** are allowed in the Cartwright Learning Resources Center.
- **Pets** are not allowed in the CLRC. (This does not include guide dogs.)
- Displaying inappropriate items is considered **misuse of computers** and will be reported to campus authorities. Examples of inappropriate items are sexually explicit, graphically disturbing, or harassing images or text.
- **Copying any software** from the computer labs is ILLEGAL. Installation of software or configuration changes on lab computers is NOT allowed.
- Do not unplug any computer station from the network. Do not plug laptops into the network.

Emerson College

http://www.emerson.edu/academic_affairs/policies/Electronic-Information-Policy.cfm

Electronic Information Policy Guidelines for Responsible and Ethical Behavior
Version 2.12 (October 16, 2000)

(This statement draws heavily upon the following documents: Ithaca College's Campus Wide Information Service Policy Statement, Bentley College's Computer Ethics Policy, SIPB Guidelines for Appropriate Use of MIT's Campus- Wide Information Services, University of Michigan's Computing Handbook, University of Missouri-Columbia Code of Conduct for Legal and Ethical Computer Use, University of Rochester's Acceptable Use Policy and User Manual, University of California - Santa Barbara's Responsible Use Policy and Harvard's Use of Computers and Networks.)

All students, faculty and staff are encouraged to choose computing resources appropriate to their work. All users of Emerson College's computing resources are expected to behave in a responsible, ethical, and legal manner. In general, appropriate use means respecting the rights of other computer users, the integrity of the physical facilities, and all pertinent and contractual agreements.

The following list, though not exhaustive, provides some specific guidelines for responsible and ethical behavior:

- Use only computers, computer accounts, and computer files for which you have authorization.
- Network services and wiring may not be modified or tampered with. This applies to all network wiring hardware and jacks.
- Network services and wiring may not be extended beyond the port provided. Retransmission or propagation of network services is prohibited without explicit permission. This includes the installation of hubs, switches and wireless equipment.
- You are ultimately responsible for anyone's use of your network connection.
- Obey established guidelines for any computers or networks used inside and outside the College.
- Do not attempt to access restricted portions of the operating system, security software, or accounting software unless authorized by the appropriate College administrator.
- Abide by all applicable laws.
- Respect the privacy and personal rights of others. Do not access or copy another user's electronic mail, data, programs, or other files without permission.
- Abide by all applicable copyright laws and licenses. Both College policies and the law expressly forbid the copying of software that has not been placed in the public domain or distributed as "freeware" or "shareware." Reproduction of copyrighted material is subject to the Copyright laws of the United States (Title 17, U.S.C.). Infringement of copyright may subject persons to fines and penalties.

- Employ appropriate standards of civility when using computer systems to communicate with other individuals.
- Be sensitive to the needs of others, and use only your fair share of computing resources. The network is a shared resource, thus network use or applications which inhibit or interfere with the use of the network and services by others are not permitted.
- Treat computing resources and electronic information as a valuable College resource. Protect your data and the systems you use.
- Use Emerson's computing facilities and services for College related work. Activities that would jeopardize the College's tax-exempt status are prohibited. Persons are not permitted to engage in consulting or other business ventures using the Emerson College network.
- The network may not be used to provide computer services or Internet access to anyone outside of Emerson College for any purposes without the express written permission of the Vice President of Administration and Finance.
- Stay informed about the computing environment.
- Take due precaution against the spread of computer viruses. Install virus protection software on your computer. Regularly check hard drive and exposed floppy disks for the presence of viruses.
- The following activities are specifically prohibited: disclosing your password to others; using somebody else's password to gain access to Emerson's system; using illegally obtained software on the system; copying, altering or deleting someone else's files without that person's permission; forging messages; cracking passwords and systems; sending harassing or threatening messages; The sending of unauthorized anonymous messages; the sending of bulk unsolicited messages; reading someone else's files without permission system attacks; denial of services; and other malicious uses of the network and systems.
- Sending data over the campus network and/or Emerson College computer systems and identifying yourself as anything but your assigned username is strictly forbidden.
- Network connections may not be used to monitor network traffic or devices by means of hardware or software applications.
- All IP addresses, both static and dynamic, are the Property of Emerson College.

VIOLATIONS OF GUIDELINES

Violations of the above policies are considered unethical and may lead to College disciplinary action and/or criminal prosecution. Individuals are encouraged to report information concerning instances in which the above guidelines have been or are being violated. In accordance with the established College practices, policies, and procedures, confirmation of inappropriate use of Emerson College technology resources may result in termination of access, expulsion from the College, termination of employment, legal action or other disciplinary action.

Questions about this document and reports of possible violation can be directed to the EIP Executive Board (send a message to EIPB@emerson.edu).

Cypress College--COMPUTER USE POLICY--Library

The Cypress College Library maintains a number of computerized research tools, including the online catalog, CD-ROM databases, and Internet workstations, all in support of the educational mission of Cypress College. We appreciate your courtesy and cooperation in the use of these resources. While using the library computing facilities, please be aware that:

- Students have priority in the use of all computers, and research needs have priority in the use of all applications
- No email, chat, games or word processing is allowed; please use one of the campus open labs for your non-research activities
- There is a 15-minute time limit for any workstation when others are waiting; web surfers will be asked to give up their stations to those who need them for research purposes
- Printing is available on most workstations at 10 cents per page
- On selected workstations, you may download free of charge to a floppy diskette, assuming no copyright or other law is broken
- Only authorized personnel are allowed to change the setup of any library computer workstation; this includes downloading files of any kind to a hard drive and/or changing desktop settings
- Unauthorized use of computing resources may result in disciplinary action on the part of Cypress College
- The library reserves the right to limit access to any and all computerized information resources. We also reserve the right to revise the terms under which these resources may be used in the course of meeting the educational needs of the Cypress College students, faculty and staff, and the community.
-

For further information about your rights and responsibilities, please read the Cypress College Computing Resources Acceptable Use Policy

COMPUTER USE POLICY

Purpose

The purpose of this document is to explain the terms of use for instructional computing resources available to students of Cypress College. All computing resources are intended to support the research and educational mission of Cypress College; their use is a privilege and a responsibility. The use of computing resources is subject to all applicable local, state and federal laws, the general guidelines outlined in this document, and any specific guidelines in effect at individual computing centers. (See NOCCCD Board Policy 10009 for more information).

Definitions

Electronic communications, electronic communication services or electronic communication systems include, but are not limited to, electronic mail, electronic mail address or account, District computer systems, Internet Services, voice mail, audio and video conferencing, and facsimile messages that are used to create, send, forward, rely to, transmit, store, hold, copy, download, display, view, read, access, or print.

Service Restrictions

Users of Computer and Electronic Communications Systems and services are expected to do so responsibly and in compliance with state and federal laws, policies and procedures of the District, and with normal standards of professional and personal courtesy and conduct. Reasons for restricting access to the electronic communications services include, but are not limited to, the following: when required by and consistent with law; when there is significant reason to believe that violations of policy or law have occurred; when failure to act my result in significant bodily harm, when significant property loss or damage would result, when loss of significant evidence of one or more violations of law or of District policies would result, when significant liability to the district or to members of the District community would result; or District business operational needs warrant. Electronic communications access privileges may not be transferred or converted to other individuals.

Access and Disclosure
Users should have no expectation of privacy or confidentiality in the content of electronic communications or other computer files sent, received, or stored.

Although the District does not routinely inspect, monitor, or disclose electronic communications, the District reserved the right to inspect, monitor, or disclose electronic communications without prior notices and without consent. Reasons for inspecting, monitoring or disclosing electronic communications include, but are not limited to, the following: when required by and consistent with law; when there is significant reason to believe that violations of policy or law have occurred; when failure to act may result in significant bodily harm, when significant property loss or damage would result, when loss of significant evidence of one or more violations of law or of District policies would result, when significant liability to the District or to members of the District community would result; or significant liability to business purposes, such as inspection of the contents of electronic messages in the course of an investigation triggered by indications of misconduct.

Users
Users of District electronic communication services are limited to District students, faculty, staff and other authorized persons.
The use of Distruct computer systems and electronic communication systems and origin, sex, sexual orientation, age, sisability, religion, or political beliefs;
Sending or accessing pornography or patently obscene material other than for authorized research or instructional purposes;
Any use that violates District policies or guidelines including, but not limited to, policies or guidelines regarding intellectual property, nondiscrimination, or sexual or other forms of harassment.

Users of the District's electronic communication services shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the District or any unit of the Distric unless appropriately authorized to do so.
False Identity

Users of the District's elenctronic communication services shall not employ a false identity or otherwise transmit or attempt to transmit any message which is misleading as to origination.

Violation of software licensing agreements, using software without obtaining legal authorization, or unauthorized duplication, transmission, or use of unlicensed copies.
Private commercial purposes not under the auspices of the District;
Personal financial gain;

Any purpose that could reasonably be expected to interfere with or disrupt use of the Electronic Communication Systems or cause, directly or indertecly, excessive strain on any computing facilities, or unsolicited interference with others' use of the system, including, but not limited to the following:
Sending or forwarding "junk" e-mail or mass electronic mailings
Exploiting list servers or similar broadcast systems
Knowingly resending the same e-mail repeatedly
Knowingly loading virus programs onto or from any computer system (viruses);
Attempting unauthorized access or alteration to data, files, passwords or breach of security measures on any electronic communication systems, or attempting to intercept, eavesdrop, record, read, receive or alter other person's e-mail without proper authorization (hacking);
Unauthorized tampering with computing resources
Policy Violations

Violations of District policies and procedures governing the use of District computer systems and electronic communication services may result in the temporary or permanent restriction of access to District computer systems and electronic communication services and appropriate with existing board policies and State Education Code. Violation of state or fedleral law may result in a referral to the appropriate law enforcement agencies.

Campus Computer Center/Labs
Individual computing centers maintain their own specific policies that supplement the Board Policy. Users of individual computing centers are to follow these policies. Computing Centers and Labs are authorized to enforce both the District/Campus Acceptable Use Policy and their own indiviual policies. Users who establish individual computer accounts for use of Internet e-mail, applications or campus resources will be required to abide by all the policies.

Users of the computer lab facilities expect to have:

an environment free of disruptive activity.
workstations that are working properly and not modified by previous use.
surroundings and workstations free from problems caused by food, beverages, and other damaging substances.