



Academic Computing & Networking

Computing & Networking Resource and Responsible Use Policies & Guidelines

Related policies, agreements, processes, and guidelines

[Campus E-Mail Policy](#)

[Campus Privacy Policy Information](#)

[Reporting Alleged Copyright Infringement](#)

[Campus Wireless Network Infrastructure Policy](#)

[Personal Home Page Policy](#)

[Network Abuse and Incident Reporting](#)

[AC&N Policy Violations Processes](#)

[Campus Network Connection & Use Policy](#)

[Housing Networking Connection & Use Policy](#)

[Network Vulnerability Scanning Policy](#)

[Comp Ctr Lab Reservation & Use Policy](#)

[CSMCC PC Software Installation Policy](#)

[Academic Dept. Support Service Level Understanding](#)

[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 e-mail 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