Acceptable Use Policy for Computing and Networking Resources

Colorado State University and the College of Health and Human Sciences

Computing and data communications at Colorado State University are valuable and limited resources that serve a large number and variety of users. All users have the responsibility to make use of these resources in an efficient, ethical, and legal manner.

The University's computer and network services provide access to resources on and off campus and shall be used in a manner consistent with the instructional, research, and administrative objectives of the University community in general and with the purpose for which such use was intended. Such open access is a privilege, and imposes upon users certain responsibilities and obligations. Access to the University's computers and network services is granted subject to University policies, and local, state, and federal laws. Acceptable use is always ethical, reflects academic honesty, and shows restraint in the consumption of shared resources. It demonstrates respect for intellectual property, protection of sensitive information, ownership of data, copyright laws, system security mechanisms, and individuals' rights to privacy and to freedom from intimidation and harassment. All activities inconsistent with these objectives are considered to be inappropriate and may jeopardize continued use of computing facilities and networks.

In consideration of being allowed to use the University's and the College of Health and Human Sciences' (CHHS) computer and network services ("Resources"), I understand and agree to the following:

1. **I shall not use the Resources for any illegal activity or for any activity prohibited by this policy (see subsequent pages for examples of inappropriate conduct that is prohibited), the "Students' Rights and Responsibilities" policy or the policies set forth in the "Academic Faculty and Administrative Professional Manual.**
2. **I agree not to use the Resources to infringe upon or otherwise impair, interfere with or violate any copyright or other intellectual property rights of another. This pertains to all copyrighted material, including, but not limited to music, video and software. I understand that I may be potentially liable for misuse of the Resources, including acts that are contrary to University policy. Except for such claims as may be covered by the Governmental Immunity Act (Colorado Revised Statutes 24-10-101 et seq.), I agree to be responsible for all claims arising from my misuse of the Resources and shall indemnify and hold harmless the University and the College from any costs, expenses or liabilities that might be asserted or imposed upon it or any of its officers, agents or affiliates as a result of such misuse.**

3. **I shall avoid any action that interferes with the efficient operation of the Resources or impedes the flow of information necessary for academic or administrative operations of the University or the College.**
4. **I shall protect my computer resources such as user accounts, passwords, and systems from unauthorized use. I acknowledge that I am responsible for reasonably securing my computer, including implementing such protections as user accounts and passwords to prohibit unauthorized use, applying in a timely fashion operating system and software patches that protect my computer from hackers, and implementing virus scanning software.**
5. **I will access only information that is my own, which is publicly available, or to which my access has been authorized. I will only access networks, network resources, and information for their intended use.**

Examples of Inappropriate Conduct:

Conduct which violates this policy includes, but is not limited to:

- Accessing another person's computer, user account, files, or data without permission.
- Using the campus network to gain unauthorized access to any computer system.
- Using any means to decode or otherwise obtain restricted passwords or access control information.
- Attempting to circumvent or subvert system or network security measures. Examples include creating or running programs that are designed to identify security loopholes, to decrypt intentionally secured data, or to gain unauthorized access to any system.
- Engaging in any activity that might be purposefully harmful to systems or to any information stored thereon, such as creating or propagating viruses, disrupting services, damaging files or making unauthorized modifications to university data.
- Performing any act, intentionally or otherwise, that will interfere with the normal operation of computers, peripherals, or networks.
- Making or using illegal copies of copyrighted software, storing such copies on any university systems, or transmitting them over university networks.
- Harassing or intimidating others via electronic mail, news groups or web pages.
- Initiating or propagating electronic chain letters.
- Initiating or facilitating in any way mass unsolicited and unofficial electronic mailing (e.g., "spamming", "flooding", or "bombing.").
- Forging the identity of a user or machine in an electronic communication.
- Saturating network or computer resources to the exclusion of another's use, for example, overloading the network with traffic such as emails or legitimate (file backup or archive) or malicious (denial of service attack) activities.
- Using the University's systems or networks for personal gain; for example, by selling access to your user account or to university systems or networks, or by performing work for profit with university resources in a manner not authorized by the University.

- Engaging in any other activity that does not comply with the general principles presented above.

Enforcement

The University considers violations of acceptable use principles or guidelines to be serious offenses. The University will take such action it deems necessary to copy and examine any files or information resident on university systems allegedly related to unacceptable use, and to protect its network from systems and events that threaten or degrade operations. Violations may be referred to the appropriate University entity for discipline.

The College of Health and Human Sciences and/or Colorado State University will use its best efforts to contact the offending party via e-mail, telephone, or in person to explain the problem and discuss its resolution before taking any action deemed necessary to protect the integrity of the Resources.

In the case of major infractions, for example those that impair others' ability to use networking and computing resources, the CHHS and/or CSU may immediately restrict systems or network access as it deems necessary to mitigate such activities. Only thereafter will CHHS and/or CSU make a reasonable effort to contact the involved parties when these incidents occur.