POLICIES OF COLORADO STATE UNIVERSITY-PUEBLO

UNIVERSITY POLICY

Policy Title: ACCEPTABLE USE POLICY FOR TECHNOLOGY RESOURCES	Policy ID #: Category: Information Technology Services Select a Category: Contact(s):
☐ Draft	x Final
☐ New Policy x Revision of Existing Policy	Effective Date: 02/06/2015

POLICY PURPOSE

Computing and data systems, equipment and services at Colorado State University-Pueblo are valuable and limited resources that serve a large number and variety of Users. Misuse of these resources can result in loss of integrity, functionality, speed, bandwidth and reliability of the University's information systems, as well as violations of other laws and policies (such as those concerning conflicts of interest). The purpose of this policy is to establish what constitutes acceptable use of these resources in order to assure that they are available to everyone as needed for the University's business needs.

APPLICATION OF POLICY

This policy applies to all users of CSU-Pueblo email systems, including students, faculty, staff, administration and affiliates.

DEFINITIONS

"Resources" include, but are not limited to, University technology devices, servers, networks, storage devices and systems (including cloud storage), data, applications, installed software, and system credentials.

POLICY STATEMENT

All Users have the responsibility to make use of the Resources in an efficient, ethical, and legal manner. The Resources are meant to be used in a manner consistent with the instructional, research, and administrative objectives of the University community in general and with the purposes for which such Resources were provided. Access to the Resources is a privilege and imposes upon Users certain responsibilities and obligations, as further described in this policy. All users must agree in writing to comply with this policy prior to being given access to University electronic resources and may need to update such agreement from time to time based on changes to the policy.

POLICY PROVISIONS

1.   Access to the Resources is granted subject to CSU System and 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 an individual's 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 the Resources. The University will take action it deems necessary to protect the Resources from systems and events that threaten or degrade operations.

2.   In consideration of being allowed to use the Resources, each User acknowledges and agrees to the following statements:

    a. I will not use the Resources for any illegal activity or for any activity prohibited by this policy or the other policies referenced herein.

    b. I will not use the Resources to infringe upon any copyright or other intellectual property rights of another. This pertains to all copyrighted material, including, but not limited to, written works, recorded music, photographs, video and software. I understand that I may be held personally liable for copyright infringement. (See References below for more information on copyright laws and policies).

    c. I understand that I am responsible for my own misuse of the Resources, and misuse by others that I knowingly permit or enable (for example, by sharing my password). I agree to be responsible for all claims arising from my misuse of the Resources and shall indemnify and hold harmless the Board of Governors and the University 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.

    d. I will 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, and will immediately discontinue such activities once I become aware of its effects.

    e. I will protect the Resources from unauthorized use and acknowledge that I am responsible for reasonably securing the Resources that have been assigned to me, including implementing such measures as outlined within the University's IT Security Policy and any related procedures and guidelines, as well as in federal and state regulations that may apply (such as FERPA or HIPAA). This also includes applying, in a timely manner, operating system and software patches, and implementing malware scanning that protects my computing device from unauthorized access. (Reference: IT Security Policy).

    f. I will only use the Resources for their intended purposes. I will only access Resources that have been authorized for my use, or which are publically available.

    g. I understand that the University retains all ownership rights to all its collective data. I acknowledge that, unless specifically authorized by a University official, copying University data to a personal device, storage location or any other media/network/resource which is beyond the University's direct control is prohibited.

    h. I understand that incidental personal use of Resources (such as email, Internet access, fax machines, printers, and copiers) is permitted only when it conforms to this policy. "Incidental use" is use that is infrequent, does not interfere with the normal performance

of my duties or the duties of another, and does not unduly delay others' use or cause the university to incur costs. Such use is restricted to approved Users only and does not include family members or others not affiliated with the University.

    i. Storage of personal email messages, voice messages, files and documents on the University's Resources must be nominal so as not to burden the university's servers and other storage devices.

3. Examples of Inappropriate Conduct Using University Resources:
Conduct which violates this policy includes, but is not limited to:

a. Accessing another person's computer, computer account, files, or data without permission.
b. Giving usernames and passwords to other persons, even temporarily.
c. Using the campus network to gain unauthorized access to any computer system.
d. Using any means to decode or otherwise obtain restricted passwords or access control information.
e. 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.
f. Engaging in any activity that might be purposefully harmful to systems or to any information stored thereon, such as creating or propagating viruses or malware, disrupting services, damaging files or making unauthorized modifications to university data.
g. Performing any act, intentionally or otherwise, that will interfere with the normal operation of computers, peripherals, or networks.
h. Making or using illegal copies of copyrighted software, storing such copies on university systems, or transmitting them over university networks.
i. Harassing or intimidating others via email, social media, news groups or Web pages.
j. Initiating or propagating electronic chain letters.
k. Initiating or facilitating in any way mass unsolicited and/or unofficial electronic mailing (e.g., "spamming", "flooding", or "bombing.").
l. Forging the identity of a User or Resource in an electronic communication.
m. Saturating network or a Resource 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.
n. Using the University's systems or networks for personal gain; for example, by selling access to your PID or to university systems or networks, or by performing work for profit with university resources in a manner not authorized by the University.
o. Engaging in any other activity that does not comply with the general principles presented above or are a violation of any other policies of the University and the Board of Governors.

I acknowledge that the Acceptable Use Policy (AUP) will change from time to time depending upon the needs of the University. I understand that I am responsible for reviewing the official version of the AUP from time to time to be sure I understand what is acceptable.

RESPONSIBILITIES

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.

In the case of major infractions, for example those that impair others' ability to use networking and computing resources, those that are a safety or security concern, or whenever necessary to protect Resources, the University may immediately restrict systems or network access as it deems necessary to mitigate such activities.

This policy is enforced when a violation is brought to the attention of the President, the Chief Information Officer or the Vice Presidents, who in turn may enforce the policy or delegate the enforcement of the policy to the appropriate persons in coordination with the disciplinary procedures for students, faculty and staff.

RELATED LAWS, POLICIES & PROCEDURES

CSU-Pueblo Email and Electronic Mass Communications Policy
CSUS Use of Digital Resources Policy – Policy 127
Faculty Handbook
Student Code of Conduct
AUP form

APPROVED:

COLORADO STATE UNIVERSITY-PUEBLO

By: _Lesley DiMare_

Lesley DiMare, President

Date: _1/22/15_