University of Colorado
Colorado Springs

UCCS CAMPUS POLICY

Policy Title: Responsible Computing

Policy Number: 700-002 **Policy Functional Area: INFORMATION TECHNOLOGY**

Effective:	November 24, 2015
Approved by:	Pam Shockley- Zalabak, Chancellor
Responsible Vice Chancellor:	AVCIT
Office of Primary Responsibility:	Information Technology
Policy Primary Contact:	Information Technology, 719-255-3536
Supersedes:	February 25, 2003; January 18, 2005; May 19, 2011
Last Reviewed/Updated:	November 24, 2015
Applies to:	UCCS Students, Faculty, Staff, and Guest

Reason for Policy: The purpose of this policy is to set forth the general principles, requirements, prohibitions, and procedures applicable to the use of UCCS Computing and Network Resources

---

I. INTRODUCTION

The University of Colorado Colorado Springs (UCCS) provides access to Computing and Network Resources for its students, faculty, staff, University of Colorado affiliates and guests to support its educational, research, public service, and administrative mission in the best possible way. Effective support of the University's mission requires complying with relevant legal, contractual, professional, and policy obligations whenever information technology resources are used. Effective support also means that individuals not interfere with the appropriate uses of information technology resources by others. This policy sets forth the general principles regarding appropriate use of equipment, software, networks and data by users of the University's Computing and Network Resources.

II. POLICY STATEMENT

A. Authority for the creation of campus administrative policies is found in the Laws of The Regents, as amended in 2007, Article 3 Section B.5, which states:

> The chancellor of each campus shall be the chief academic and administrative officer responsible to the president for the conduct of the affairs of their respective campus in accordance with the policies of the Board of Regents. The chancellor shall have such other

responsibilities as may be required by these Laws or regent policy, or as may be delegated by the president.

B. Procedures:

1. Access and Use of Computing and Network Resources

a. Passwords

All Authorized Users are issued a username and password in order to access UCCS Computing and Network Resources. Usernames and passwords also may be given out to be used for specific Computing and Networking Resources. Prohibited behaviors include, but are not limited to, the following:

i. Disclosing their password to another person, either intentionally or unintentionally, except as required for a legitimate business purpose.
ii. Taking any action to discover, intercept, or decode others' passwords.
iii. Misrepresenting (including forgery) the identity of the sender or source of an electronic communication.
iv. Acquiring or attempting to acquire passwords of others.
v. Using or attempting to use the computer accounts of others.
vi. Altering the content of a message originating from another person or computer with intent to deceive.
vii. Running or otherwise configuring software or hardware to allow access to Computing and Network Resources by unauthorized users.

b. Authorized Uses of Computing and Network Resources

UCCS Computing and Network Resources are for the use of Authorized Users only and for use only in a manner consistent with each user's authority.

Authorized uses of Computing and Network Resources include those uses that are consistent with the instructional, public service, research, and administrative objectives of the University. Use should also be consistent with the specific objectives of the project or task for which such use was authorized.

c. Prohibited Uses of Computing and Network Resources

UCCS Computing and Network Resources may not be used in any manner inconsistent with a user's authority or as prohibited by licenses, contracts, University policies, or local, state, or federal law. No one may grant permission for inappropriate use of Computing and Network Resources, nor does the ability to perform inappropriate actions constitute permission to do so. Prohibited uses of UCCS Computing and Network Resources include, but are not limited to, the following:

i. Any use for commercial purposes or personal financial gain.
ii. Any use for political advocacy, such as supporting or opposing political campaigns, candidates, legislation, or ballot issues.

iii. Any use that violates University or third party copyright, patent protections, or intellectual property.
iv. Any use that seeks to interfere with the intended use of Computing and Network Resources or that seek to gain unauthorized access to Computing and Network Resources.
v. Any use that is abusive, threatening, discriminatory, defamatory, or harassing towards others.
vi. Any use that damages, alters, or compromises the integrity of Computing and Network Resources.
vii. Any use that purposely denies appropriate access to other users.
viii. Any use that violates any University policy, or local, state, or federal law, including any student activity that is prohibited pursuant to the Student Code of Conduct.

d. Incidental Personal Use

Computing and Network Resources may be used for incidental personal use so long as such use does not generate a direct cost for UCCS. Incidental personal use of Computing and Network Resources must adhere to all university policies and must not involve violations of the law, interfere with the fulfillment of education and/or employment responsibilities, or adversely impact or conflict with activities supporting UCCS' educational mission.

e. Commercial Use

Under special circumstances, and only with the approval of the Executive Director of Information Technology, UCCS Computing and Network Resources may be used for commercial purposes if those purposes have been determined compatible with the mission of the University.

2. Registration of Servers:

The Department of Information Technology (IT) at UCCS supports and maintains a number of servers for general campus usage. All servers connected to UCCS campus network that provide information resources intended to be used by others must be registered with the UCCS Department of Information Technology. This includes all web servers located outside of the IT department.

3. Privacy:

UCCS will make reasonable efforts to maintain the integrity and effective operation of its Computing and Network Resources, but users are advised that those systems should in no way be regarded as a secure medium for the communication of sensitive or confidential information. Because of the nature and technology of electronic communication, the University cannot assure either the privacy or the confidentiality of an individual user's use of the University's Computing and Network Resources. Users should have no expectation of privacy concerning the use of University's technology resources. Confidential data that is maintained by University personnel and stored or transmitted on Computing and Network Resources is to adhere to the policy of the Information Security

Program - APS 6005. Responsibilities for the protection of data by University employees are outlined in Information Security Program - APS 6005.

In addition, Colorado law provides that electronic records constitute writings for purposes of Colorado's Public Records Act, C.R.S. 24-72-201, *et seq*. and may be considered public records subject to public inspection. Exceptions to what must be made available for public inspection under the Public Records Act may be found in Appendix A of APS 2022 - Colorado Open Records Act.

4. Monitoring and Access:

During normal operation, network and system monitoring may be used to protect University data. The Department of IT may monitor user activities and access any files or information in the course of performing normal system and network maintenance or while investigating possible violations of laws or policy. Anyone using UCCS Computing or Network Resources expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, IT will provide the evidence to law enforcement or University officials.

5. Violations:

Any actions that violate this policy, including violations of Section V, will be addressed by the University and may result in disciplinary action, up to and including expulsion and/or termination of employment, regardless of whether UCCS Computing or Network Resources or other resources were involved in their commission. Any individual who knows or suspects that UCCS Computing or Network resources have been used in a manner which may be in violation of University policy, or federal, state, or local law should immediately notify abuse@uccs.edu.

The Chancellor delegates authority to the UCCS Department of Information Technology or the University of Colorado Office of Information Security to investigate alleged violations in consultation with the Office of University Counsel. The department conducting the investigation may also consult with the Human Resources Department, the Office of Institutional Equity and/or the Office of the Dean of Students, as applicable. During an investigation, it may be necessary to temporarily suspend a user's network or computing privileges. Upon conclusion of the investigation, a user's network or computing privileges will be restored, subject to possible sanctions and/or sanction recommendations as described below.

Sanctions may be administered by the Department of Information Technology. Depending on the alleged violation and the respondent's relationship with the University, sanctions may also be administered by an appointing authority and/or the Dean of Students for violation of University policy. Such sanctions include, but are not limited to, any one or a combination of the following: suspension of internet access, suspension of email privileges, suspension of computing privileges, suspension, expulsion, exclusion, employment termination from the University, as well as those sanctions under the

Student Code of Conduct for student violations.

Allegations of illegal activity in possible violation of state and/or federal law may result in civil and/or criminal penalties and will be referred to appropriate law enforcement personnel for separate investigation.

C. Responsibility:

All UCCS faculty, staff, students, student-employees, retired faculty and staff, and those individuals who have been given permission to access UCCS Computing and Network Resources are responsible for compliance with this policy.

III. KEY WORDS

A. Authorized Users
B. Computing and Network Resources

IV. RELATED POLICIES, PROCEDURES, FORMS, GUIDELINES, AND OTHER RESOURCES

A. Administrative Policy Statements (APS) and Other Policies
   1. University of Colorado Administrative Policy Statement, APS 6002- Electronic Communications
   2. University of Colorado Administrative Policy Statement, APS 6005- IT Security Program
   3. University of Colorado Administrative Policy Statement, APS 5014 Sexual Misconduct
   4. UCCS Policy 700-001: Email as Official Means of Communication
   5. UCCS Student Code of Conduct

B. Procedures

C. Forms

D. Guidelines

E. Other Resources (i.e. training, secondary contact information)

F. Frequently Asked Questions (FAQs)

V. HISTORY

Initial policy approval	February 25, 2003
Revised	January 18, 2005
Revised	May 19, 2011