CENTRAL ARIZONA COLLEGE

College Policy

Category:	Institutional Rules and Regulations
Policy Number:	515
Policy Title:	Computer and Network Use
This Policy Adopted On:	04/21/1998
Revised Date:	

Central Arizona College computing, telecommunications, and networking resources are provided for the support of instruction, administration, and research activities of the institution. These resources are to be used for College business only and users are required to conduct their activities within the restrictions of College Policies, laws of the State of Arizona, and federal statutes. Misuse of Central Arizona College computing facilities, telecommunications or networking systems or associated facilities, resources or equipment includes:

1. Damage of computing facilities, programs, or data.
2. Access to, or copying of, computing facilities or programs without proper authorization.
3. Allowing the reproduction of copyrighted material in any form without proper authorization.
4. Use of computing facilities, programs, or data which are not authorized to the user's account.
5. Sharing access codes or any security-related procedure, file, or account with other individuals.
6. Intentionally rendering computer systems, telecommunications, facilities, networks, or other resources inoperative, e.g., "crashing" the system.
7. Use of computing systems, telecommunications facilities, networks, or other resources for political or commercial activity.
8. Use of computing systems, telecommunications, facilities or networks to abuse, defame, harass or threaten another individual or group, commit fraud or distribute other unlawful messages.
9. Use of computer systems, telecommunications facilities, networks, or other resources for frivolous or pornographic purposes.
10. Any other uses of college computing resources which are not in the best interest or part of the normal business of Central Arizona College.

Central Arizona College will take action against a user who willfully misuses computer resources. Such actions may include canceling the user's account, revoking the user's operating privileges, revoking access to resources, assessing discipline in accordance with applicable College Policy, and seeking prosecution under the laws of the State of Arizona.

A completed user agreement must be on file with the College before a user's account numbers will be established. The College reserves the right to access and monitor all messages and files on the College system. Users should not assume electronic communications are private and are to transmit confidential data in other ways.

CENTRAL ARIZONA COLLEGE

College Procedure

Category:	Institutional Rules and Regulations
Procedure Number:	515
Procedure Title:	Computer and Network Use
Revised Date:	05/07/2004

Appropriate use of CAC e-mail, telecommunications, and Internet services is the responsibility of every student, faculty member, staff member, or anyone else who uses CAC information resources. Those who use these resources are expected to do so responsibly and in compliance with state and federal laws, with the policies and procedures of CAC, and with normal standards of professional conduct and personal courtesy.

CAC e-mail, telecommunications, and Internet services are intended to be used to support legitimate college business. Personal use of these services is permitted but such use must be brief and occasional, and it must conform to the restrictions set forth in subsequent paragraphs of this policy document.

Requirements and Prohibited Use

Users of CAC Computing and Communications Resources agree to:

1. Comply with all applicable local, state, and federal laws and regulations, and with CAC Policies.
2. Respect academic freedom and free speech rights.
3. Be truthful and accurate in personal and computer identification.
4. Respect the rights and privacy of others, including intellectual property and personal property rights.
5. Respect the integrity of CAC's electronic networks, avoid restricted areas, and refrain from activities that may damage the network, or transmitted or stored data.
6. Maintain the security of accounts and protect and regularly change their account passwords. Individuals responsible for system administration are required to change passwords regularly to protect information and maintain security.

Prohibited Uses of CAC Computing and Communications Resources

The following activities are not allowed:

1. Engage in unlawful communications, including threats of violence, obscenity, child pornography, and harassing communications.
2. Use College-owned or leased computer equipment "to access, download, print, or store any information, infrastructure, files, or services that depict nudity, sexual activity, sexual excitement, or sexual acts" unless the employee has written approval from the "agency head" (Arizona State Law, ARS § 38-448). At Central Arizona College, the agency head is the Chief Executive Officer or the CEO's designee.

3. Make personal use of the Internet and e-mail services in a way that impedes or interferes with the conduct of College business. In general, only incidental amounts of employee time—time periods comparable to reasonable coffee breaks during the day—should be used to attend to personal matters.

4. Employ CAC computer resources for private business or commercial activities, fund-raising, or advertising on behalf of non-CAC organizations. Nor are they permitted to engage in the unauthorized reselling of CAC computer resources or the unauthorized use of College trademarks or logos.

5. Place links on the College Website that generate or have the potential to generate revenue to CAC or any private business (including *click trade* or banner advertising) without the approval of Senior Administration. Note that this is not a general prohibition against links to commercial Websites.

6. Alter addresses, uniform resource locator (URL), or take other action that masks the Centralaz.edu domain as a host site.

7. Intercept or attempt to intercept communications by parties not authorized or intended to receive them or general unauthorized anonymous and pseudoanonymous communications.

8. Misrepresent or forge the identity of the sender or the source of an electronic communication; unauthorized acquisition, attempts to acquire, or use of another person's password or the computer account of others.

9. Modify or delete another person's files or account or alter the content of a message originating from another person or computer with intent to deceive.

10. Compromise the privacy or security of electronic information through an intentional or reckless manner or make CAC computing resources available to individuals not affiliated with CAC without approval of an authorized CAC official.

11. Deliberately interfere with or disrupt computer or network accounts, services, or equipment of others**,** propagate computer "worms" and "viruses," send electronic chain mail, or send "broadcast" messages to large numbers of individuals or hosts that are not College related.

12. Disrupt electronic networks through negligent or intentional conduct; attempt to alter any CAC computing or networking components (including, but not limited to, bridges, routers, and hubs) without approval; or damage through intentional conduct CAC electronic information, computing/networking equipment.

<u>Electronic Mail and Electronic Communications</u>

Conditions for Restriction of Access to Electronic Mail

Access to CAC e-mail is a privilege that may be wholly or partially restricted without prior notice and without consent of the user:

1. If required by applicable law or policy;

2. If a reasonable suspicion exists that there has been or may be a violation of law, regulation, or policy;

or

3. If required to protect the integrity or operation of the e-mail system or computing resources or when the resources are required for more critical tasks as determined by appropriate management authority.

Conditions for Permitting Inspection, Monitoring, or Disclosure

CAC may permit the inspection, monitoring, or disclosure of e-mail, computer files, and network connections when:

1. Required or permitted by law, including public records law, or by subpoena or court order;

2. CAC or its designated agent has reason to believe that a violation of law or policy has occurred;

or

3. It is necessary to monitor and preserve the functioning and integrity of the e-mail system or related computer systems or facilities.

All computer users agree to cooperate and comply with CAC requests for access to and copies of e-mail messages or data when access or disclosure is authorized by this policy or required or allowed by law or other applicable policies.

Prohibition Against Activities Placing Strain on Facilities

Activities that may strain the e-mail or network facilities more than can be reasonably expected are in violation of this policy. These activities include, but are not limited to: Sending chain letters; "spam," or the widespread dissemination of unsolicited e-mail; and "letter bombs" to resend the same e-mail repeatedly to one or more recipients.

Electronic Mail as Arizona Public Record

Electronic information produced in the course of College business is considered an Arizona public record, and must be stored or deleted in accordance with Arizona public records law.

Privacy and Security

Right to Examine Computers and Equipment

College owned computers and equipment are the property of CAC and as such may be accessed:

1. To solve technical problems;
2. During the course of an investigation;
3. To detect illegal software;
4. To evaluate the security of the network; or
5. To check on other issues related to the use or abuse of the system.

Employees, students or others authorized to access and use CAC computers, e-mail or telecommunications systems should not expect that voice mail messages, e-mail messages or other forms of communication are private.

Violations and Enforcement

Reporting Violations

Any actual or suspected violation of the rules listed above should be brought to the attention of the Chief Information Officer.

CAC Response to a Reported Violation

Upon receiving notice of a violation, CAC may temporarily suspend a user's privileges or move or delete the allegedly offending material pending further proceedings.

A person accused of a violation will be notified of the charge, at the appropriate time, and will have an opportunity to respond before CAC imposes a sanction. In addition to sanctions available under applicable law and CAC policies, CAC may impose a temporary or permanent reduction or elimination of access privileges to computing and communication accounts, networks, CAC administered computing rooms, and other services or facilities.

Applicable Law and Policies

CAC students and employees are bound by all applicable law and College policies.