

# APPROPRIATE USE OF COMPUTING EQUIPMENT - 1-18A – Revised June 2001

## I. Purpose

To ensure the proper use of computing equipment in accordance with the mission of the College of Eastern Utah and the guidelines of its academic and administrative environment. The College creates and maintains computing and networking equipment for the purpose of conducting and supporting the instructional and research activities of students, faculty, and staff.

## II. Definitions

Equipment - any College owned computer equipment (hardware, software, and/or network capabilities) or computer equipment using the College system.

Systems Administrator - one whose job description requires the individual to maintain, repair, and/or have access to the College computer system.

## III. Rights and Responsibilities

Use of the College's computer system must be in accordance with and adhering to institutional policies and procedures, and must be consistent with the College's mission.

### A. Individual users must:

1. Obey federal, state, and campus policies and regulations which govern computer and telecommunication use.
2. Accept that instructional, administrative, and research uses of system resources take priority over all other uses.
3. Consent to the interception of all network traffic, including e-mail, by System Administrators under circumstances where there is imminent danger to life, safety, health, security, property, or operations.
4. Recognize that user actions reflect on both the user and the institution.
5. Protect the privacy of self and others.
6. Choose safe passwords, change them often, and do not disclose them.
7. Keep accounts stored on the server free of non-essential files.
8. Backup all private, important, or irreplaceable files.
9. Inform the licensing administrator (the computer lab supervisor at the Price campus or the Information Technology Manager at the San Juan Campus) of any and all software installed by the user on a College computer and provide appropriate licensure information.

### B. System Administrators must:

1. Enforce sanctions of this policy in cooperation with appropriate authorities.
2. Perform routine maintenance of the systems, including keeping a backup of information on networked file servers (not responsible for lost data due to system errors).
3. Treat the contents of files as private and confidential.
4. Perform periodic security checks to ensure that computing resources of the College are as secure as the College can make them.
5. Disclose e-mail messages, files, backups, and any other pertinent records only to authorized law enforcement officials or other authorized third parties.

### C. Users and System Administrators must not:

1. Attempt to gain access to any system or account without permission from the appropriate System Administrator (if necessary).
2. Share passwords and/or accounts.
3. Copy or change system files or software without authorization.
4. Use destructive or invasive software.
5. Violate licensing agreements, patent, copyright, and/or trademark laws.
6. Display images, sounds, or messages which are obscene.
7. Crash machines or systems deliberately, participate in electronic chain letters, or use the College computing equipment for disruptive or illegal activities.

## IV. Security

It is intended that all computing resources owned and managed by the College be as secure as the College can make them. Users who find possible security breaches should report them to their System Administrator as soon as possible. A security breach is any unauthorized use of an account, unauthorized access or unauthorized changes to system resources, or attempting to acquire another person's password. Any use of the system under the breach conditions is prohibited. Users should not share their accounts with anyone. Passwords are never to be given or shared with others, and should not be words or terms that are easily guessed (like spouse's name, birth date, phone number). Bad passwords diminish the integrity of the system and may lead to security breaches. Passwords should be changed often.

## V. Privacy

Employee files are public documents. See GRAMA (Government Records Access and Management Act). Consequently, files may be subject to inspection through the GRAMA office (Office of Academic Records/Registrar). In such cases, the College GRAMA officer has authority to inspect files to determine which portions may be exempt from disclosure. Any inspection of electronic files, and any action based upon such inspection, will be governed by all applicable federal and state laws, and College policy. Routine maintenance of systems occasionally results in files being read. Network and System Administrators are required to treat the contents of electronic files as private and confidential, but users should exercise caution with confidential information. It is the intent of the College that the e-mail on the system be as private as possible. Attempts to read another person's e-mail (or other protected files) will be treated with the utmost seriousness. The System Administrators will not read mail or other electronic media files unless absolutely necessary in the course of their duties, and will treat the contents of those files as private information at all times. Violation of an individual's right to privacy by a System Administrator could jeopardize that Administrator's employment with the College.

## APPROPRIATE USE OF COMPUTING EQUIPMENT - 1-18A – Revised June 2001

### VI. Free Expression

Communications which originate from the College's equipment are free from censorship or prior restraint, except when they are illegal or against policy. Academic institutions exist for the transmission of knowledge and the pursuit of truth. Censorship of material on partisan or doctrinal grounds is contrary to these goals. Interfering with the freedom of expression of others is unacceptable.

### VII. Electronic Mail (E-Mail)

E-mail is an inappropriate vehicle for the transmission of information which needs to remain secure from disclosure. Users should expect that nothing delivered or received via e-mail is private. The College is obligated to disclose e-mail messages to law enforcement officials or others authorized under GRAMA without prior notice. Users are responsible for the contents of their accounts. E-mail messages normally should not be retained for more than one semester. Users who feel that they need to retain copies of messages beyond that time should archive them, save them to a file, or print a hard copy of them.

### VIII. Violations and Penalties

Use of the College computing equipment and accounts is a privilege. Violation of the College policy or federal, state, and/or local law may lead to the revocation of computing privileges. Violations of this policy will be referred to the appropriate academic, administrative, and/or legal authority. System Administrators are authorized to disable accounts when violations occur. Grievances may be filed in accordance with the College's Policies and Procedures Manual (see policy 3-11, Grievance Procedure).

Utah law (76-8-703 to 705) prohibits interfering with the peaceful conduct of the activities of the College or disruption of the school or its students or activities. Examples include, but are not limited to, software programs or activities which are destructive, harmful, troublesome, ruinous, devastating, vicious, invasive, encroaching, infringing, trespassing, or interfering.

#### A. Pertinent laws include, but are not limited to:

1. Copyright - Software available on computers and networks is not to be copied in violation of any copyright or any applicable software license.
2. Harassment - A course of conduct directed at a specific person that causes emotional distress in such person and serves no legitimate purpose.
3. Threats -Federal law prohibits threats. Whoever transmits through interstate commerce any communication containing any threat to kidnap a person or any threat to injure the person of another will be fined or imprisoned, or both.
4. Libel-Utah law (76-9-502) prohibits libel. Persons are guilty of libel if they intentionally and with a malicious intent to injure another publish or procure to be published any libel. Libel

damages the memory of one who is dead, or impeaches the honesty, integrity, virtue, or reputation, or publishes the natural defects of one who is alive, thereby exposing him/her to public hatred, contempt, or ridicule.

5. Disorderly Conduct - Utah law (76-9-102) prohibits a person from knowingly creating a hazardous or physically offensive condition by an act which serves no legitimate purpose, intending to cause public inconvenience, annoyance or alarm, or recklessly creating a risk thereof.
6. Public Displays - Utah law (75-10-1228) prohibits public display (at any establishment frequented by minors, or where the minors are invited as a part of the general public, i.e. the College), any motion picture, or any still picture that consists of nude or partially denuded figures posed or presented in a manner to provoke or arouse lust or passion.
7. Pyramid Schemes -Utah law (76-6a-3) prohibits organizing, establishing, or administering pyramid schemes. Pyramid schemes are defined in Utah law (76-6a-3) as "any sales device or plan under which a person gives consideration to another person in exchange for compensation or the right to receive compensation which is derived primarily from the introduction of other persons into the sales device or plan rather than from the sale of goods, services, or other property."
8. Pornography - Individuals using College computing equipment are prohibited from viewing pornographic material. Pornographic material is defined by Utah law (76-10-1203) using the following criteria:
  - a. The average person, applying contemporary community standards, finds that, taken as a whole, it appeals to prurient interest in sex;
  - b. It is patently offensive in the description or depiction of nudity, sexual conduct, sexual excitement, sadomasochistic abuse, or excretion; and
  - c. Taken as a whole it does not have serious literary, artistic, political or scientific value.
  - d. In prosecutions under this part, where circumstances of production, presentation, sale, dissemination, distribution, exhibition, or publicity indicate that the matter is being commercially exploited by the defendant for the sake of its prurient appeal, this evidence is probative with respect to the nature of the matter and can justify the conclusion that, in the context in which it is used, the matter has no serious literary, artistic, political, or scientific value.

### IX. Review

At least annually, the Institutional Technology Committee will evaluate changes in law and technology which impact the College.