POLICY TITLE	Appropriate Use of Computing Facilities	Policy Number	441
Section	Facilities, Operations, and Information Technology	Approval Date	June 13, 1996
Subsection	Information Technology	Effective Date	June 13, 1996
Responsible Office	Office of the Vice President of Information Technology		

1.0 PURPOSE

1.1 UVU creates and maintains computing and networking facilities for the purpose of conducting and supporting the instructional and research activities of students, faculty, and staff. This policy was designed and implemented to ensure the proper use of computing facilities in accordance with the mission of the University and the guidelines of its academic and administrative environment.

1.2 The growth of the Internet and the freedom of information exchange were key factors in the design of this policy. Many academic and administrative bodies were involved in the creation of the policy including the Network Policies Subcommittee, Information Technology Committee, President's Staff, Faculty Senate, Student Government, and PACE.

1.3 UVU endorses the following statements:

1) The Educom Code for Software and Intellectual Rights was developed through Educom, a non-profit consortium of colleges and universities committees to the use and management of information technology in higher education, and the Information Technology Association of America (ITAA), a computer software and services industry association. As follows:

a) Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to works of all authors and publishers in all media. It encompasses respect for the right to acknowledgment, right to privacy, and right to determine the form, manner, and terms of publications and distribution.

b) Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environments. Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorized access, and trade secret and copyright violations, may be grounds for sanctions against members of the academic community.

2) An excerpt for the Joint Statement on Rights and Freedoms of Students created by the American Association of University Professors (AAUP) pertaining to student due process in the event of a circulation of this policy:

a) Pending action on the charges, the status of a student shall not be altered, or his right to be present on the campus and to attend classes suspended, except for reasons relating to the student's physical or emotional safety and well-being, or for reasons relating to the safety and well-being of students, faculty, or university property.

2.0 REFERENCES

2.1 18 U.S.C. 875

2.2 413 U.S. 15, 93 1973

2.3 Utah law 76-8-703 to 705, 76-9-502, 76-9-102, 76-10-1228, 76-6a-3, 77-23a-1 to 16, 77-23a-4 or 77-23a-9

2.4 UVU Policy 156 *Grievances*

2.5 UVU Policy 203 *Purchasing*

2.6 UVU Policy 541 *Student Rights and Responsibilities Code*

2.7 UVU Policy 647 *Faculty Grievance*

2.8 AAUP Policy Statement

2.9 "Banning 'Indecency'—Colleges Weigh Impact of Proposed Restrictions on Internet Material," *Chronicle of Higher Education,* January 5, 1996 (A19).

2.10 *Black Law Dictionary*, 6th Edition

2.11 *The Chronicle of Higher Education* (ongoing)

2.12 "Colleges Criticized for Response to Offensive Electronic Speech," *Chronicle of Higher Education,* December 1, 1995 (A32).

2.13 "Colleges Oppose Proposed Ban on 'Indecent' Material Online," *Chronicle of Higher Education,* December 15, 1995 (A24).

2.14 Computer Freedom and Privacy Conference 1995 & 1996

2.15 "Discovery of E-Mail and Other Computerized Information" by Heidi McNeil and Robert M. Kort in *Arizona Attorney* (April 1995).

2.16 "Electronic Communications" in *Perspective: The Campus Legal Monthly* (October 1995).

2.17 Electronic Frontier Foundation Policy on Computer Use

2.18 "E-Mail Institutional Liability, and Freedom of Expression" in *Synfax Weekly Report* (April 25, 1994).

2.19 "E-Mail Policies Are Crucial for University E-Mail Users," Item #12 from NACUA Conference by Richard Raysman (June 1995).

2.20 "'Fantasies' on the Internet" in *Synfax Weekly Report* (March 13, 1995).

2.21 The Fifth Conference on Computers, Freedom and Privacy (March 1995)

2.22 "The Web in the Workplace," *The Net,* January 1996 (12).

3.0 DEFINITIONS

3.1 Crash: A disruption of the supervisory or accounting functions of the computing facilities or doing anything which is likely to have that effect.

3.2 Disruptive activities: Utah law (76-8-703 to 705) prohibits interfering with the peaceful conduct of the activities of the University or disruption of the school or its students or activities. Examples include, but are not limited to software or activities which are:

3.2.1 Destructive: Harmful, troublesome, ruinous, devastating, vicious.

3.2.2 Invasive: Encroaching, infringing, trespassing, interfering.

3.3 Due Process: As with other policies at the University, both notice and hearing are provided. Because of the unique nature of computing facilities, notice of a problem with one's account may be provided by disabling the account. The user then has the opportunity to discuss with the affected system administrator what prompted that action. If the user is dissatisfied with the response from the system administrator, then the user may exercise his/her grievance rights. Grievance policies are provided for users according to whether they are students, faculty, or staff.

3.4 Illegal activities: Pertinent laws include, but are not limited to:

3.4.1 Copyright infringement: Software available on computers and networks is not to be copied in violation of any copyright or any applicable software license.

3.4.2 Harassment: A course of conduct directed at a specific person that causes emotional distress in such person.

3.4.3 Threats: Federal law prohibits threats.18 U.S.C. 875 states: Whoever transmits in interstate commerce any communication containing any threat to kidnap a person or any threat to injure the person of another shall be fined not more than $1,000 or imprisoned not more than five years, or both.

3.4.4 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 or her to public hatred, contempt, or ridicule.

3.4.5 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. Making unreasonable noises in a public place. Engaging in abusive or obscene language or making obscene gestures in a public place.

3.4.6 Public displays: Utah law (76-10-1228) prohibits public display (at any establishment frequented by minors, or where the minors are invited as a part of the general public, i.e. UVU), 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.

3.4.7 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 or other persons into the sales device or plan rather than from the sale of goods, services, or other property."

3.4.8 Obscenity: Objectionable or offensive to accepted standards of decency. The test: whether the average person, applying contemporary community standards would find that the work, taken as a whole, appeals to the prurient, whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law, and whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value. See, Miller v. California (413 U.S. 15,93 1973), the U.S. Supreme Court case which clarified the term "obscene"

3.5 **Inordinate:** Determined by affected system administrators. Including, but not limited to: affecting available disk space, CPU time, e-mail system, printing facilities, and dial-up access lines.

3.6 Interception: Utah law (77-23a-1 to 16) allows for interception of communications.

3.6.1 The University, as a provider of electronic communications service, may provide information/technical assistance to persons authorized by law to intercept communications if the University is provided with a court order or certificate from the Attorney General's office that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required.

3.6.2 University system administrators may intercept electronic communications if one of the parties to the communication has given prior consent to the interception (unless it is intercepted to commit a crime or a tort) or if the electronic communication is made through a system that is readily accessible to the public.

3.6.3 University system administrators may divulge the contents of any communication:

1) As authorized under Utah Law 77-23a-4 or 77-23a-9;

2) With lawful consent of the originator or any addressee or intended recipient of the communication;

3) To a person employed or authorized or whose facilities are used to forward the communication to its destination;

4) Inadvertently obtained by system administrators and to pertain to the commission of the crime (contents can then be revealed only to law enforcement).

3.7 Passwords: Are never to be given to other people, shall not be easily guessed, and shall be frequently changed. Bad passwords can create security breaches. Change a bad password when notified by a system administrator. Failure to do so will result in the account locked. Examples of bad passwords are those:

1) Related to the user (like phone number, birth date, spouse name).

2) Easily guessed by a system administrator (in fewer than five tries).

3.8 Responsible for the contents of their accounts: Includes, but is not limited to: Having incoming mail held/forwarded when off campus for extended periods of time, emptying trash, deleting outbox messages which are no longer needed, and archiving messages to be saved.

3.8.1 Messages shall not be retained beyond one term. Users who feel the need to retain copies of messages beyond that point need to archive them, save them, or print them and retain them in that form.

3.8.2 Users shall categorize messages when they are created. Note whether they are privileged or what future value they have so that they can be more readily archived and referenced.

3.9 Routine maintenance of the system: Includes, but is not limited to: Security checks, deletion of temporary files, verification of e-mail delivery, and assurance of available disk space.

3.10 Security breach:

3.10.1 Unauthorized use of an account.

3.10.2 Unauthorized access or unauthorized changes to system resources.

3.10.3 Using bad passwords, or attempting to use or acquire others' passwords.

3.11 Security check: Verification that privacy is ensured and access is granted as needed and appropriate.

3.12 System files: Any files that control or otherwise affect the startup or operation of a computer system.

4.0 POLICY

4.1 Ensure the proper use of computing facilities maintained by the University for instructional, administrative, and research activities of students, faculty, and staff. Reviewed at least annually, the Computing Policy Committee, a standing subcommittee of the InfoTech Committee, shall evaluate changes in law and technology which impact the University. The committee shall invite representatives of UVUSA, PACE, and Faculty Senate to participate.

4.2 Rights and Responsibilities

4.2.1 Use of the UVU computer system must be legal, ethical, and consistent with the University's mission.

4.2.2 Individual users must:

1) Choose safe passwords, change them often, and do not disclose them.

2) Keep accounts free of cluttering files.

3) Backup all private, important, or irreplaceable files.

4) Accept that instructional, administrative, and research uses of system resources take priority over all other uses.

5) Obey federal, state, and local laws which govern computer and telecommunication use.

6) Consent to the interception of e-mail by system administrators under circumstances where there is imminent danger to life, safety, health, security, or property.

7) Recognize that user actions reflect on both the user and the University.

8) Protect the privacy of self and others.

9) Perform personal file maintenance (including scanning for viruses and deleting unnecessary files regularly).

4.2.3 System administrators must:

1) Perform periodic security checks to ensure that computing resources provided by the University are as secure as the University can make them.

2) Treat the contents of files as private and confidential.

3) Perform routine maintenance of the system.

4) Keep a backup of information on networked file servers, but have no responsibility for lost data due to system errors.

5) Enforce violations of this policy in cooperation with appropriate authorities.

6) Disclose e-mail messages, files, backups, and any other pertinent records to authorized law enforcement officials or other authorized third parties.

4.3 Prohibitions

4.3.1 Users must not:

1) Attempt to gain access to any system or account without authorization from a system administrator.

2) Share passwords and/or accounts.

3) Copy or change system files or software without authorization from a system administrator.

4) Use destructive or invasive software.

5) Violate licensing agreements, patent, copyright and/or trademark laws or UVU Purchasing regulations as governed by UVU Policy 203 *Purchasing*.

6) Display images, sounds, or messages which are obscene where others may be affected by them.

7) Consume inordinate amounts of system resources.

8) Crash machines or systems deliberately.

9) Participate in electronic chain letters.

10) Reserve shared resources. A public shared computing facility device left unattended for more than ten minutes is available for use, and any process running at the time of abandonment shall be terminated. Running unattended programs or placing signs on devices to "reserve" them is inappropriate without authorization from a system administrator.

11) Lock a public shared workstation or computer without authorization from a system administrator.

12) Use the University computing facilities for disruptive or illegal activities.

4.4 Violations and Penalties

4.4.1 Use of UVU computing facilities and accounts is a privilege.

4.4.2 Violation of UVU policy or federal, state, and/or local law may lead to revocation of computing privileges.

4.4.3 Violations of this policy are referred to the appropriate academic, administrative, and/or legal authority. System administrators are authorized to disable accounts when violations occur.

4.4.4 Due process is afforded users charged with violations.

4.4.5 Grievances may be filed.

4.4.5.1 Students see UVU Policy 541 *Student Rights and Responsibilities Code*

4.4.5.2 Faculty see UVU Policy 647 *Faculty Grievance*.

4.4.5.3 Staff see UVU Policy 156 *Grievances*.

4.5 Security

4.5.1 All computing resources owned and managed by UVU are as secure as the University can make them.

4.5.2 Users who find possible security breaches shall report them. Any use of the system under the possible security breach condition is prohibited.

4.5.3 Users are responsible not to share passwords or their accounts.

4.5.4 Bad passwords jeopardize security.

4.6 Privacy

4.6.1 Employee files are public documents. See *GRAMA* (*Government Records Access and Management Act*). Consequently, files may be subject to inspection through the GRAMA office. In such cases, the university GRAMA officer has authority to inspect files to determine which portions may be exempt from disclosure.

4.6.2 Any inspection of electronic files, and any action based upon such inspection, shall be governed by all applicable federal and state laws, and university policy.

4.6.3 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 shall exercise caution with confidential information.

4.6.4 E-mail on the University system is as private as possible. Attempts to read another person's e-mail (or other protected files) shall be treated with the utmost seriousness. The system administrators shall not read mail or other electronic media files unless absolutely necessary in the course of their duties, and shall treat the contents of those files as private information at all times.

4.6.5 Students who wish to have their personal information removed from directory databases need to contact the Records office, and submit appropriate authorization.

4.7 Free Expression

4.7.1 Communications which originate from UVU facilities are free from censorship or prior restraint, except when they are illegal.

4.7.2 Universities exist for the transmission of knowledge and the pursuit of truth. Censorship of material on partisan or doctrinal grounds is contrary to these goals.

1) Downloading: Academic library standards and principles of intellectual property are applied to material received from computer networks.

2) Publishing: Faculty and student intellectual and academic freedom standards are applied to publication in computer media.

3) Interfering with the freedom of expression of others is unacceptable.

4.8 Electronic Mail (E-Mail)

4.8.1 Users are responsible for the contents of their accounts.

4.8.2 Employee e-mail messages are university records (see *GRAMA*).

4.8.3 E-mail is an inappropriate vehicle for the transmission of personal and/or confidential information which needs to remain secure from disclosure. Users shall expect that nothing delivered or received via e-mail is private.

4.8.4 The University is obligated to disclose E-mail messages to law enforcement officials, or others authorized under *GRAMA*, without prior notice.

4.8.5 Prohibited E-Mail

1) Illegal messaging.

2) Electronic chain letters

3) Mailbox contents which consume inordinate amounts of system resources.

4) Only University Marketing and Communications may send messages to the entire faculty, staff, and administration. Those wishing to reach all faculty, staff, and administration must do so through University Marketing and Communications ' weekly *UVAnnounce*.

5) To send unsolicited messages to large groups of people, seek authorization from University Marketing and Communications in advance.

POLICY HISTORY		
Date of Last Action	Action Taken	Authorizing Entity