

SUBJECT: Use of Information Technologies and Resources	Effective Date: 5-21-08	Policy Number: 4-002
	Supersedes:	Page Of 1 6
	Responsible Authority: Vice Provost for Information Technologies and Resources	

APPLICABILITY/ACCOUNTABILITY:

This policy applies to all University of Central Florida students, employees, and others who use university information technologies and resources.

POLICY STATEMENT:

The University of Central Florida's computing and telecommunications resources provide a wide range of capabilities for students and employees to communicate, store, and process information that is essential to the academic, research, and administrative functions of the university. It is the policy of the University of Central Florida that all students and employees use these resources described in the procedures below.

DEFINITIONS:

Computing resource. Personal computers, laptops, and portable computing and communication devices, servers, mainframes, data storage systems, and similar equipment capable of processing, accessing, displaying, or communicating electronic information.

E-mail. For purposes of this policy, e-mail includes point-to-point messages, postings to newsgroups and listservs, and any electronic messages involving computers and computer networks.

Electronic information resource. Data or information in electronic format and the computing and telecommunications resources through which such resources are accessed or used.

Telecommunications resource. Wired or wireless voice or data communications circuits or networks and associated electronic equipment.

Departmental Security Coordinator. A designated departmental employee who coordinates the use, and management of departmental computer resources and access to university administrative computing systems on behalf of their department.

User. A person who makes use of or accesses university computing, telecommunications, or electronic information resources.

BACKGROUND:

Computer accounts are provided to students and employees as a privilege associated with membership in the university community and with varying access rights according to institutional role.

UCF students and employees are generally free to use UCF computing, telecommunications, and electronic information resources as necessary to carry out their assigned responsibilities, subject to the authorized use of those resources as described in this policy.

The university has the right to disconnect or remove university or privately-owned equipment or restrict use thereof at any time as required to maintain the functionality, security, or integrity of university computing and telecommunications resources.

This policy is not intended to abridge academic freedom or the constitutional guarantees of freedom of speech or freedom of expression.

PROCEDURES:

A. User Responsibilities

1. Users are responsible for any activity originating from their accounts that they can reasonably be expected to control. Accounts and passwords must not be shared with others.
2. Computer users shall comply with all applicable user conduct codes and rules, laws, and regulations governing the use of computer and telecommunications resources. Examples include the laws of libel, privacy, copyright, trademark, obscenity, child pornography, the Florida Computer Crimes Act, the Electronic Communications Privacy Act, and the Computer Fraud and Abuse Act.
3. Except in isolated or occasional circumstances, the computing and telecommunications resources of the university shall be used only for purposes directly related to or in support of the academic, research, or administrative activities of the university. If a university employee wishes to use university facilities, students, equipment, materials, or software for personal or outside professional purposes, permission must be obtained in advance using form AA22 (faculty members) or HR-12 (A&P or USPS).
4. Users shall not attempt to undermine the security or the integrity of computing systems or telecommunications networks and shall not attempt to gain unauthorized access to these

resources. Users shall not employ any computer program or device to intercept or decode passwords or similar access control information. If security breaches are observed or suspected, they must be immediately reported to the appropriate system administrator, departmental security coordinator, or the university information security officer.

5. Users shall not use computer or telecommunication systems in such a manner as to degrade or disrupt the normal operation of voice or data networks or university computer systems or to intentionally damage or disable computing or telecommunications equipment or software.
6. Users shall ensure that software acquisition and utilization adheres to the applicable software licenses and U.S. copyright law. Users shall maintain documentation sufficient to prove that all software installed on any computer workstation assigned to them has been legally obtained and is installed in conformance with the applicable license(s). Backup copies of software shall be made only if expressly permitted by the applicable license(s).
7. To maintain proper functioning of computer and networking hardware and software, system administrators and individual users shall take reasonable care to ensure their computing facilities are free of viruses or other destructive software through installation and frequent updating of antivirus and antimalware software.
8. Users of university computing facilities and telecommunications networks shall use these resources prudently and avoid making excessive demands on these facilities in a manner that would knowingly impair access to or use of these resources by others.

B. Use and Misuse of Computing and Telecommunications Resources

1. The university's computing and telecommunications resources shall not be used to impersonate another individual or misrepresent authorization to act on behalf of other individuals or the university. All messages transmitted through university computers and telecommunications networks must correctly identify the sender.
2. The computing and telecommunications resources of the university shall not be used to make unauthorized or illegal use of the intellectual property of others, including copyrighted music, videos, films, and software.
3. The computing and telecommunications resources of the university shall not be used for unapproved commercial purposes or for personal financial gain without express written approval from the Provost and Executive Vice President or his or her designee.
4. Users shall not transmit to others or intentionally display in the workplace images, sounds, or messages that could reasonably be perceived as harassing, invasive, or otherwise unwanted.

5. Users shall not use university computer or telecommunications resources to download, intentionally view, store or transmit images that could reasonably be regarded as obscene or pornographic.
6. The university provides telephone systems and long distance services for official university business. University employees are allowed to make incidental use of the telephone system for necessary personal calls but must reimburse the university for any tolls or other charges incurred through personal use.
7. The university provides e-mail and other electronic messaging systems only for official university business. University employees are allowed to make incidental use of such systems for necessary personal messaging. The following uses of university messaging systems by students and employees are prohibited under this policy:
 - a. chain letters
 - b. harassing or hate messages
 - c. threatening or abusive e-mail sent to individuals or organizations that violates university procedures and regulations
 - d. virus hoaxes
 - e. spamming or e-mail bombing attacks (intentional high volume e-mail transmissions other than officially approved campus general mailings)
 - f. “phishing” messages
 - g. commercial use or personal financial gain
 - h. unsolicited e-mail that is not related to university business
 - i. false identification (any messages that misrepresent or fail to accurately identify the true originator.)
 - j. messages that contain or direct users to computer viruses, worms, or other harmful software
 - k. any illegal activity or crime
8. The university and its employees are prohibited from using any university resources in support of a political campaign or for campaign fund raising, even under a reimbursement arrangement. An example of prohibited use would be a university employee using university e-mail or Web or telephone resources to solicit support of a political candidate or to raise funds for a candidate.

C. Access to and Disclosure of Electronic Information

1. Users should be aware that their uses of university computing and telecommunications resources are not completely private. The university does not routinely or without cause monitor individual use of these resources; however, the normal operation and maintenance

of these resources require the backup and caching of data and communications, logging of activity, monitoring of general usage patterns, and other such activities that are required to manage these services. In addition, information stored on university computing resources or passed through university telecommunications networks may be accessible to the public through public record laws, subpoenas, interception, or other means.

2. The university may specifically monitor the activity or accounts of individual users of university computing and telecommunications resources, including individual login sessions and the content of individual communications, without advance notice when:
 - a. the user has voluntarily made such information accessible to the public, as by posting to a listserv, blog, or Web page
 - b. it reasonably appears necessary to do so to protect the integrity, security, or functionality of university or other computing resources or to protect the university from liability
 - c. there is reasonable cause to believe that the user has violated or is violating this policy
 - d. an account appears to be engaged in unusual or excessive activity
 - e. it is otherwise required or permitted by law
3. Access to and disclosure of electronic information shall be governed by the following provisions.
 - a. Professional ethics dictate that any person having access to proprietary or confidential information shall:
 - 1) use that access only to the extent required to discharge the assigned responsibilities of that person's position
 - 2) not disclose any such information except to the extent authorized or required under this policy or applicable rules or laws
 - 3) not use, in any manner, such information or knowledge for personal gain
 - b. A university employee may not read, view, listen to, or otherwise access electronic messages or the contents of computer systems without the knowledge or consent of the user except under the circumstances provided for in this policy or upon express prior authorization from the Provost and Executive Vice President, his or her designee, or the General Counsel. Such prior authorization shall be given in writing and must clearly state the purpose of granting such access. Information accessed in authorized instances shall not be disclosed except as provided in this policy or with prior written authorization from the university's Provost and Executive Vice President, his or her designee, or the General Counsel. Such prior authorization to disclose shall be given only in cases involving an actual or possible breach of system security, a violation of law, a violation of university rule or policy, or dereliction of duty or responsibility on the part of a university user.

- c. It is the responsibility of each person having access to proprietary or confidential information to pursue any case of actual or suspected abuse or misuse of university computing and telecommunications resources. Proper pursuit of such cases may require that person to disclose relevant information to supervisors or designated investigators.

D. Enforcement

1. Violations of computer and network procedures and policies shall result in disciplinary action, in accordance with applicable student, faculty, and staff handbooks, the disciplinary provisions of all applicable university collective bargaining agreements in place at the time such violation occurs, Florida Administrative Code, University Regulations, and the Digital Millennium Copyright Act of 1998. Violations of university policies shall be referred to the appropriate university official(s) for disciplinary actions. Suspected criminal violations of Federal, State, or local laws shall be reported to the university police, the university auditor's office, or any other applicable authorities or agencies.
2. Unauthorized or fraudulent use of university computing or telecommunications resources can result in felony prosecution as provided for in Florida Statutes.
3. Any violation of the policy and procedures described above may result in immediate loss of network and computer access privileges, seizure of equipment, or removal of inappropriate information posted on university-owned computers or university-supported Internet sites or pages.

RELATED DOCUMENTS:

The following related policies are available online at: <http://www.policies.ucf.edu/>

Policy 2-100 *Florida Public Records Act—Scope and Compliance*

Policy 2-103 *Use of Copyrighted Materials*

Policy 4-001 *Retention Requirements for Electronic Mail*

Policy 4-006 *Broadcast Distribution of Electronic Mail*

Policy 4-007 *Security of Mobile Computing, Data Storage, and Communication Devices*

Policy 4-008 *Data Classification and Protection*

Permission to Use UCF Personnel, Equipment, Facilities, Students, or Services Form AA22 (Faculty) <http://www.facultyrelations.ucf.edu/Forms/AA22.pdf>

Permission to Use UCF Personnel, Equipment, Facilities, Students, or Services Form HR-12 (A&P, USPS) <http://hr.ucf.edu/web/forms/employeerelations/useofpefss.pdf>

INITIATING AUTHORITY: Provost and Executive Vice President

POLICY APPROVAL (For use by the Office of the President)	
Policy Number: 4-002	
Initiating Authority: <u>[Signature]</u>	Date: <u>7/22/08</u>
Policies and Procedures Review Committee Chair: <u>[Signature]</u>	Date: <u>July 21, 2008</u>
President or Designee: <u>[Signature]</u>	Date: <u>7/25/08</u>

