University of Central Florida

Office of the President

SUBJECT:	Effective Date:	Policy Number:
	9/1/2016	4-002.2
Use of Information Technologies and Resources	**Supersedes:** 4-002.1	**Page** 1 **Of** 8
	Responsible Authority: Vice President for Information Technologies and Resources	

DATE OF INITIAL ADOPTION AND EFFECTIVE DATE 5/21/2008

APPLICABILITY/ACCOUNTABILITY

This policy applies to all University of Central Florida students, employees, and others who use university information technology 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 ethically, responsibly, and in compliance with all applicable federal and state laws, university policies, and as prescribed by this policy's procedures.

Any violation of this policy and procedures 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. In addition to these corrective actions, failure to comply with this policy and procedures may result in disciplinary action up to and including termination.

DEFINITIONS

Computing Resource. Personal computers, laptops, and portable computing and communication devices, such as tablets, and smartphones, servers, mainframes, data storage systems, and similar equipment capable of processing, accessing, displaying, storing, or communicating electronic information.

Credentials. A combination of user name, password, and possibly additional information such as a PIN or biometric scan that together are required to access a computer system or information resource.

Departmental Security Coordinator. A designated employee who serves as the primary contact between the respective department or business unit and the Information Security Office (ISO) for all matters relating to information security.

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

Electronic Messages. For purposes of this policy, electronic messages include electronic mail, text messages, videos, images, or sound files that are sent from a computing resource through a computer network.

Internet Cloud Storage. Data stored in third party data centers, e.g., CrashPlan, Dropbox, iCloud, Google Drive, OneDrive, Box, etc.

Restricted Data. Any confidential or personal information that is protected by law or policy and that requires the highest level of access control and security protection, both in storage or in transit. Further defined in UCF policy 4-008.1 *Data Classification and Protection*.

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

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 and job duties.

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 and other UCF

policies. The university reserves 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. Credentials must not be shared with others.

2. Users shall comply with all applicable user conduct codes and rules, laws, and regulations governing the use of computer and telecommunications resources. Examples include laws regarding libel, privacy, copyright, trademark, obscenity, and 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, service, 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 AA-21 (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, and 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 sufficient

documentation to prove that all software installed on any computing resource assigned to them was legally obtained and is installed in conformance with the applicable license(s). Backup copies of software may 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 resources are free of viruses or other malicious software through installation and frequent updating of antivirus and antimalware software, and frequent updates of operating systems and applications.

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 computing resources 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, texts, images, 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 are reminded of the university's commitment to a civil and non-discriminatory environment. Employees, including student employees, shall not transmit to others or intentionally display in the workplace materials or messages that could reasonably be perceived as invasive of another's privacy; pornographic; harassing; or disruptive to the operations of the university or any part thereof.

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 toll calls incurred through personal use that exceed $90 per year, per Policy 4003.1.

7. The university provides email 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 messages sent to individuals or organizations
    d. messages that include malware, phishing, or hoaxes
    e. spamming or high volume email transmission other than those specifically allowed by the Broadcast Distribution of Electronic Mail Policy (4-006.1)
    f. for commercial use or personal financial gain
    g. false identification (any messages that misrepresent or fail to accurately identify the true originator)
    h. messages that contain or direct users to computer viruses, worms, or other harmful software
    i. 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 electronic messaging 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. 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 a university policy, a regulation, or a law
d. an account appears to be engaged in unusual or excessive activity
e. it is otherwise required by subpoena or court order

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 restricted 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 of another user without the knowledge or consent of that user, except: (i) under the limited circumstances provided for in this policy or (ii) upon express prior authorization from the provost and executive vice president, his or her designee, the general counsel, or the UCF Police Chief or designee. 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, the general counsel, or the UCF Police. 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 regulation or policy, or dereliction of duty or responsibility on the part of a university user.

c. Any suspected abuse or misuse of university computing and telecommunications resources should be reported to the Information Security Office (407-823-3863 or

infosec@ucf.edu). Proper pursuit of such cases may require that person to disclose relevant information to supervisors or designated investigators.

d. Employees who access restricted data are expected to sign the UCF Confidentiality Agreement.

RELATED DOCUMENTS

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

Policy 2-100.4 *Florida Public Records Act—Scope and Compliance*
Policy 2-103.2 *Use of Copyrighted Materials*
Policy 4-001.1 *Retention Requirements for Electronic Mail*
Policy 4-003.1 *Telecommunications Services*
Policy 4-006.1 *Broadcast Distribution of Electronic Mail*
Policy 4-007 *Security of Mobile Computing, Data Storage, and Communication Devices*
Policy 4-008.1 *Data Classification and Protection*

Potential Outside Activity, Employment, and Conflict of Interest and Commitment Disclosure (AA-21): http://compliance.ucf.edu/conflict-of-interest/

A&P and USPS Permission to Use UCF Personnel, Equipment, Facilities, Students, or Services: http://hr.ucf.edu/files/HR12_PermissionToUseServices.pdf

UCF Confidentiality Agreement: http://www.hr.ucf.edu/files/ConfidentialityAgreement.pdf

INITIATING AUTHORITY Provost and Executive Vice President

POLICY APPROVAL
(For use by the Office of the President)

Policy Number: 4-002.2

Initiating Authority: Joel C. Wachman Date: 8·31·16

University Policies and
Procedures Committee Chair: Rhonda L Bishop Date: 8/30/16

President or Designee: John C. Hitt Date: 9/1/16

History 4-002 5/21/2008, 4-002.1 5/13/2014