	COLLEGE of CENTRAL FLORIDA ADMINISTRATIVE PROCEDURE

Title: Appropriate Use Procedure	
Page 1 of 5	Implementing Procedure For Policy # 3.25
Date Approved: 02/23/05 Revised: May 2019	Division: Information Technology

Purpose

This document establishes procedures for the appropriate use of computer systems, telephone systems, networks, data, computer programs and other information technology and communication resources including the Internet and e-mail, in an appropriate, ethical, and professional manner by students, faculty, and staff ("Users") at the College of Central Florida.

User Responsibilities

Users are expected to use computer, network, and communication resources in a responsible manner for college educational or job-related purposes only and not for personal convenience. Users should take appropriate precautions to ensure the security of their passwords and prevent others from obtaining access to their computer resources. Convenience of file or printer sharing is not a sufficient reason for sharing computer accounts.

Internal and external e-mail, voice mail, and social media (for those employees authorized to maintain a college business related social media account), are considered business records and may be subject to public records requests for information and to discovery in the event of litigation. Employees must be aware of this possibility when communicating electronically within and outside the College. Only the employee's official college email address should be used when conducting business. An employee shall not use their personal email nor text messaging or social media accounts to conduct official college business.

Users may not encroach on others' use of computer resources regardless if on the College's hardwired or wireless networks. Such actions include, but are not limited to, utilizing computer resources with trivial applications or game playing, sending frivolous or excessive messages including chain letters, junk mail, and other similar types of broadcast messages, downloading or streaming pictures, music, videos, and social media unrelated to specific educational or job-related business purposes, or using excessive amounts of storage.

The following behaviors are prohibited while using College information technology and communication resources, including computers and networks owned or operated by the College of Central Florida, or to which the College of Central Florida is connected:
- Modifying system or network facilities, or attempting to hack, probe, or crash systems, servers, or networks;
- Using, duplicating, or transmitting copyrighted material, without first obtaining the owner's permission, in any way that may reasonably be expected to constitute an infringement, or that exceeds the scope of a license, or violates other contracts;
- Tampering with software protections or restrictions placed on computer applications or files;
- Using College information technology and communication resources for personal purposes unrelated to a specific education or College related business purpose and any illegal

activities—including piracy, cracking, extortion, blackmail, copyright infringement and unauthorized access to any computers on the Internet or e-mail;

- Installing unlicensed software on College computers;
- Transmitting, retrieving, or storing any communications or other content of a defamatory, discriminatory, harassing, or pornographic nature. No messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes, or sexual preference may be transmitted;
- Harassment and disparaging, abusive, profane or offensive language of any kind is prohibited;
- Sending, disseminating, or storing on a third-party provider (e.g. Google Docs, Dropbox, or other cloud storage) any College data or information that would be considered sensitive, protected, or confidential, unless it is specifically required by a State or Federal governmental body;
- Subverting restrictions associated with computer accounts;
- Using information technology resources to obtain unauthorized access to records, data, and other forms of information owned, used, possessed by, or pertaining to the College or individuals;
- Accessing another person's computer account without permission. Users may not supply false or misleading data, or improperly obtain another's password to gain access to computers or network systems, data or information. Obtaining access to an account name or password through the negligence or naiveté of another is considered to be a specifically prohibited use;
- Intentionally introducing computer viruses, Trojan Horses, or other rogue programs into information technology resources that belong to, are licensed to, or are leased by the College of Central Florida or others;
- Physically damaging information technology resources;
- Using, or encouraging others to use, information technology resources in any manner that would violate this or other College policies or any applicable state or federal law;
- Falsely reporting or accusing another of conduct that violates this policy, without a good faith basis for such an accusation; and,
- Releasing any information stored in college systems to others outside of the college except where specifically authorized to do so.

Users should remember that information distributed through the College's information technology resources might be considered a form of publication. Although the College of Central Florida does not take responsibility for material issued by individuals, users must recognize that third parties may perceive anything generated at the College of Central Florida as in some manner having been produced under the College of Central Florida auspices. Accordingly, users are reminded to exercise appropriate language, behavior, and style in their use of information technology resources.

Users must strictly adhere to software licensing agreements and copyright laws. All software licenses for software not centrally maintained by Information Technology must be on file in the department where the software is installed.

College's Right to Monitor and Consequences for Misuse

All college-supplied technology, including computer systems, equipment and college-related educational and work records, belongs to college and not to the Users. Users understand the college routinely monitors use patterns, and Users should observe appropriate discretion in their use and maintenance of such college property.

Because all the computer systems and software, as well as e-mail and Internet connections are the property of the college, all college policies apply to their use and are in effect at all times. Any User who abuses the college-provided access to e-mail, the Internet, other electronic communications, or the wireless and hardwired networks, including social media (in instances where a User is authorized to maintain a college educational or business related social media account), may be denied future access, and, if appropriate, be subject to disciplinary action up to and including termination from employment or expulsion from enrollment, within the limitations of any applicable federal, state or local laws.

E-mail and other electronic communications transmitted by the College's equipment, systems and networks are not private or confidential, and they are the property of the College. Therefore, the College reserves the right to examine, monitor, and regulate e-mail and other electronic communications, directories, files and all other content, including Internet use, transmitted by or stored in its technology systems, whether onsite or offsite, and whether via the wireless or hardwired networks. Monitoring examples include, but are not limited to:

- Enforcing policies against harassment and threats to the safety of individuals;
- Protecting against or limiting damage to College information technology resources;
- Complying with a court order, subpoena or other legally enforceable discovery request;
- Investigating and preventing the posting of proprietary software or electronic copies of texts, data, media, or images in disregard of copyright, licenses, privacy, or other contractual or legal obligations or in violation of law;
- Safeguarding the integrity, stability, and the appropriate use of computers, networks, software and data;
- Upgrading or maintaining information technology resources;
- Protecting the College or its employees and representatives against liability or other potentially adverse consequences.

Misuse of computing, networking, or information resources may result in the loss of computing and/or network access. Additionally, misuse can be prosecuted under applicable statutes. Users may be held accountable for their conduct under any applicable College or campus policies, or procedures. Illegal production of software and other intellectual property protected by U.S. copyright law is subject to civil damages and criminal punishment including fines and imprisonment.

Minor infractions of this policy, when accidental, such as consuming excessive resources, overloading computer systems, or employee loafing, are generally resolved informally by the unit administering the accounts or network. This may be done through electronic mail or in-person discussions and education.

Repeated minor infractions or misconduct that is more serious may result in the temporary or permanent loss of computer access privileges or the modification of those privileges. More serious violations include, but are not limited to unauthorized use of computer resources, attempts to steal passwords or data, unauthorized use for copying of licensed software, repeated harassment, repeated or excessive loafing, and threatening behavior, may result in termination of employment if the user is an employee or referral to an administrator for appropriate disciplinary action if the user is a student.

Violations will normally be handled through the College's disciplinary procedures applicable to the relevant user. For example, students will be investigated and penalties or discipline imposed consistent with the procedures described in college policy and the Student Code of Conduct. However, the College may deny or restrict access to resources prior to the initiation or completion of such procedures when it reasonably appears necessary to do so to protect the integrity, security, or

functionality of the resources or to protect the College from liability. The College may also refer suspected violations of law to appropriate law enforcement agencies.

Questions Regarding the Use of Technology

If you have questions regarding the appropriate use of electronic communications equipment or systems, including e-mail, wireless networks, shared network folders, and the Internet, please contact your supervisor, manager, or the College's Information Technology department.

Vice President, Administration and Finance	Date

Approved by President	Date

I have received training on the College of Central Florida's Appropriate Use Policy and Procedures for Information Technology Resources. I accept the conditions described in the Policy and Procedures.

_____

Name of Employee

_____

Title

_____

Assigned Department

_____

Employee ID Number

_____

Signature of Employee

_____

Date