	Florida Gulf Coast University Policy Manual	**Policy**: 3.022 **Approved:** 9/03/09
	TITLE: **TECHNOLOGY ACCEPTABLE USE POLICY AND PROCEDURE**	**Responsible Executive(s)**: VP for Administrative Services and Finance and Provost and VPAA **Responsible Office**: Information Systems, University Telecommunications, and Technology Support Services

I. POLICY STATEMENT

Florida Gulf Coast University's information technology resources are a vital component of the teaching, research and business environment of FGCU. It is the responsibility of all in the University community to use these resources in a responsible, legal and ethical manner.

II. REASON FOR POLICY

The purpose of this policy is to provide employees with guidance on the appropriate and inappropriate use of technology resources at FGCU.

III. DEFINITION OF TERMS

A. *Technology Resources* - All electronic devices, software, and means of electronic communication, whether provided or supported by the University, including, but not limited to, the following: personal computers and workstations, laptop computers, servers, computer hardware such as disk drives, flash drives and tape drives, peripheral equipment such as printers, modems, fax machines, and copiers, computer software applications and associated files, data and data storage systems, including software that grants access to external services, such as the Internet, equipment capable of processing, accessing, displaying or communicating electronic information, including electronic mail, telephones, cellular phones, pagers, and voicemail systems.

B. *User* - A person who makes use of or accesses University technology resources.

IV. PROCEDURES

A. Introduction

As part of its educational mission, the University acquires, develops, manages, and maintains its technology resources such as computers, computer systems, networks, web sites, cellular phones, pagers, voicemail and telephones. These technology resources are intended for University-related purposes, including direct and indirect support of the University's instruction, research and service missions, University administrative functions, student and campus life activities, and the free exchange of ideas within the University community and among the University community and the wider local, national, and world communities.

B. Application

This policy applies to all Users of University technology resources, whether affiliated with the University or not, and to all uses of those resources, whether on campus or from remote locations. Additional policies may govern specific computers, computer systems or networks provided or operated by specific units of the University.

C. Rights & Responsibilities

The rights of academic freedom and freedom of expression apply to the use of the University's technology resources, as do the responsibilities and limitations associated with those rights. The University supports a campus and technology environment open to the free expression of ideas, including unpopular points of view. However, the use of University technology resources, like the use of other University-provided resources and activities, is subject to the requirements of legal and ethical behavior. Thus, legitimate use of a computer, computer system or network does not extend to whatever is technically possible. Moreover, this policy prohibits the use of University-provided equipment for obscene or improper purposes.

D. Procedure

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. University students and employees are generally free to use University technology, 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, systems, files or web sites or restrict use thereof at any

time as required to maintain the functionality, security, or integrity of University technology resources.

E. Privacy

1. Users should also be aware that their uses of University technology resources, particularly its technology resources, are not completely private. While the University does not routinely monitor individual usage of its technology resources, the normal operation and maintenance of the University's technology resources require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns and other such activities that are necessary for the provision of service. The University may also specifically monitor the activity and accounts of individual Users, including individual login sessions and the content of individual communications, without notice, when:

    a) The User has voluntarily made them accessible to the public, as by posting to a Web page;

    b) It reasonably appears necessary to do so to protect the integrity, security, or functionality of University or other technology 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 unusually excessive activity; or

    e) It is otherwise required or permitted by law.

2. Any such monitoring of communications, other than what is made accessible by the User, required by law, or necessary to respond to perceived emergency situations, must be authorized in advance by the appropriate Vice President in consultation with the Office of General Counsel. The University, in its discretion, may disclose the results of any such general or individual monitoring, including the contents and records of individual communications, to appropriate University personnel or law enforcement agencies and may use those results in appropriate University disciplinary proceedings. Communications made by means of University technology resources are also generally subject to the Florida Public Records Law to the same extent as they would be if made on paper.

F. Deleted Information

Deleting or erasing information, documents, or messages maintained on the University's Technology Resources is, in most cases, ineffective. All employees should understand that any information kept on the University's Technology Resources may be electronically recalled or recreated regardless of whether it may have been "deleted" or "erased" by an employee. Because the University periodically backs-up all files and messages, and because of the way in which computers re-use file storage space, files and messages may exist that are thought to have been deleted or erased. Therefore, employees who delete or erase information or messages should not assume that such information or messages are confidential.

G. 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. Users shall comply with all applicable User conduct codes and rules, laws, and regulations governing the use of technology resources. Examples include, but are not limited to, the laws of libel, privacy, copyright, trademark, 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 technology 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 from their supervisor.

4. Users shall not attempt to undermine the security or the integrity of technology systems or telecommunications networks and shall not attempt to gain unauthorized access to these technology 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.

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 technology or telecommunications equipment or software.

6. All software in use on the University's technology resources must be officially licensed software. No software is to be installed or used that has not been duly paid for and licensed appropriately for the use to which it is being put. No employee may load any software on the University's computers, by any means of transmission, unless authorized in writing in advance by the appropriate University official.

7. 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). Contractual agreements related to software acquisition and utilization must be reviewed by the Office of the General Counsel, as well as approved and signed by the appropriate authorized FGCU personnel.

8. To maintain proper functioning of computer and networking hardware and software, system administrators and individual Users shall take reasonable care to ensure their computers are free of viruses or other destructive software through installation and frequent updating of antivirus and antimalware software as directed by Computing Services.

9. Users of University technology resources 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.

H. Use and Misuse of Technology Resources

1. Occasional personal use of University technology resources is permitted when it does not consume a significant amount of time or University resources, does not interfere with the performance of the User's job or other University responsibilities, and is otherwise in compliance with this policy.

2. The University's technology 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.

3. The technology 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.

4. The technology resources of the University shall not be used for unapproved commercial purposes or for personal financial gain without express written approval from the President or the President's designee.

5. The University provides telephone systems and long distances 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. Records are kept of all calls made from and to a given telephone extension.

6. Users shall not transmit to others or intentionally display in the workplace images, sounds, or messages that inhibit the ability of others to perform their job functions, or violate the University's Non-Discrimination and Anti-Harassment Regulation FGCU PR1.003. Violations of this policy may result in disciplinary action consistent with FGCU PR-5.016 and other relevant University regulations.

7. Unauthorized use of University technology resources can be a crime under the Florida Computer Crimes Act (Chapter 815, Florida Statutes), the Florida Communications Fraud Act (§817.034, Florida Statutes), the Computer Fraud and Abuse Act (18 U.S.C. 1030), as well as violate other laws, including but not limited to, libel, privacy, copyright, trademark, and child pornography. Employees must comply with all applicable laws or be in violation of this Policy.

I. Enforcement

Users who violate this policy may be denied access to University technology resources and may be subject to other penalties and disciplinary action, including possible expulsion or dismissal. Alleged violations will be handled through the University disciplinary procedures applicable to the User. The University may suspend, block or restrict access to an account, independent of such procedures, when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of University or other technology resources or to protect the University from liability. The University may also refer suspected violations of applicable law to appropriate law enforcement agencies.

V. HISTORY

New 3/2/1988; Amended 1/30/2006; 09/03/09

APPROVED	*s/Wilson G. Bradshaw	9/3/09
	President	Date

**NOTE: This policy reflects changes to the formatting only. No changes have been made to the text.*