College Operating Procedures (COP)	FLORIDA SOUTHWESTERN STATE COLLEGE

Procedure Title:	Technology Acceptable Use
Procedure Number:	02-0405
Originating Department:	Technology Services
Specific Authority:	
Board Policy	6Hx6:2:00
Florida Statute	1001.65
Florida Administrative Code	Chapter 815 – Computer Crimes Act
Procedure Actions:	
	Adopted: 6/9/09; 6/01/10; 7/24/12
Purpose Statement:	
	The purpose of this document is to establish and promote the ethical, legal, and secure use of computing and electronic communications for the Florida SouthWestern State College community.

Guidelines:

Florida SouthWestern State College (College) acquires, develops, and maintains software, computers, computer systems, and networks for College-related purposes as part of its infrastructure. The College's computing resources and infrastructure are made available to users in support of the College's instructional, research, community service missions, its administrative functions, its student and campus life activities and to promote the free exchange of ideas among members of the College community and between the College community and the wider local, national, and international communities. This acceptable use policy governs the use of these al of the College computing resources and infrastructure. This policy applies to all users of the College's computing resources and infrastructure, whether or not affiliated with the College, and also to all uses of those resources, whether from on campus or from remote locations.

Procedures:

I. **Rights & Responsibilities**

The College is committed to intellectual and academic freedom, the diversity of values and perspectives inherent in an academic institution, and to applying those freedoms to the use of its computing resources and infrastructure. However, as with any other College furnished resource, the use of its computing resources and infrastructure is subject to the normal requirements of legal and ethical behavior within the College Community. Thus, the legitimate use of these resources does not extend to whatever is technically possible.

Although some limitations may be built into computer operating systems, software, or networks, those limitations are not the sole restrictions on what is permissible. Users must abide by all applicable restrictions, whether or not built into the operating systems, software, or networks and whether or not they are capable of being circumvented by technical means.

II. Prohibited Activities

Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory or otherwise unlawful or inappropriate may not be sent by email or other form of electronic communication or displayed on or stored in the the College computers. Users encountering or receiving this kind of material should immediately report it to their supervisor or to the District Director, Human Resources. Students should report this kind of material to the Vice President of Student Services.

Students, faculty and staff may use their personal equipment to connect wirelessly to the Student Wireless System. Students, faculty and staff may not connect their personal equipment to the network wall outlet connections without first receiving written permission from the Manager – Networks and Security in the Information Technology department at the College.

Students, faculty and staff may not employ any software on the College network which disrupts other computers within or outside the College.

III. Basic Requirements

A. Eligibility Requirements

General Users are students that are currently enrolled or have attended a course(s) in the previous two terms or current non-temporary employees that have an active position at the College. Access is terminated when these eligibility requirements are no longer met.

Special Users are certain organizations and individuals that are affiliated with the College or are temporarily working with the College under the explicit ownership of an administrative or academic department. Access for special users must be approved by the District Director of Information Technology and users will only receive privileges for a period specified at the outset.

B. All users must comply with all applicable local, state, federal and foreign laws, all generally applicable College rules, policies, procedures and all applicable contracts and licenses.

These include, for example, the laws on libel, privacy, copyright, trademark, obscenity, the College Sexual Harassment Policy 05-0103, and child pornography; the Florida Computer Crimes Act (. Chapter 815, Florida Statutes), the Florida Security of Communications Statute (Chapter 934, Florida Statutes), the Electronic Communications Privacy Act (18 U.S.C. §§ 2510 et seq.), and the Computer Fraud and Abuse Act (18 U.S.C. §1030 et seq.) [Which prohibit "hacking", "cracking" and similar activities]; the **Florida SouthWestern State College Student Code of Conduct**; and all applicable software licenses. Users who interact with others in different states or countries should also be aware that they may also be subject to the laws of those other states or countries, as well as the rules and policies applicable to other systems or networks.

C. Users may use only those computing resources for which they are authorized, and use them only in the manner and to the extent authorized. Respect the privacy of other users and their accounts, regardless of whether those accounts are securely protected.

The ability to access computing resources, at the College or elsewhere, does not necessarily imply authorization to do so. Users are responsible for ascertaining what authorizations are necessary and for obtaining them before using College computing resources.

Users are responsible for any activity originating from their accounts which they can reasonably be expected to control. Accounts and passwords may not, under any circumstances, be used by persons other than those to whom they have been assigned by the Information Technology Department. In cases when unauthorized use of accounts or resources is detected or suspected, the account owner should change the password and report the incident to the Information Technology.

D. Users should respect the finite capacity of the College's computing resources and infrastructure, and avoid interfering unreasonably with the activity of other users. Although there is no set bandwidth, disk space, CPU time, or other limit applicable to all uses of College computing resources, the College may require users of those resources to limit or refrain from specific uses if, in the opinion of Information Technology, such use interferes with the efficient operations of the system.

The College may establish limits on bandwidth, disk space, usage times or other aspects of usage of its computing resources and infrastructure, with which users must comply. Additionally, users may be required to refrain from

certain specific activities which adversely impact the operation of the College's computing resources and infrastructure.

Users should refrain from using the College's computing resources for any personal use that would consume a significant portion of those resources, or interfere with the College's operations or the performance of the individual user's job or other responsibilities to the College.

IV. Security and Privacy

A. The College is also committed to protecting the privacy and integrity of computer data and records belonging to the College, individual users, and commercial providers. The College employs a variety of means to protect the security of its computing resources and infrastructure. Users should be aware, however, that the College cannot guarantee such security. Users should therefore engage in responsible computing practices by establishing access restrictions for their accounts where appropriate, guarding passwords, and changing passwords regularly.

B. Users do not own accounts on College computers, but are granted the privilege of the use of their accounts. Use of the network does not alter the ownership of data stored on the network. Users should also be aware that their use of the College's computing resources and infrastructure is not completely private. While the College does not routinely monitor individual usage of its computing resources or infrastructure, the normal operation and maintenance of those resources requires the backup and caching of data and communications, logging of activity, monitoring general usage patterns, and other such activities. The College may also specifically monitor the activity and accounts of individual users of its computing resources, including individual login sessions and communications, without notice, when (a) the user has voluntarily made them accessible to the public, as by posting to a Listserv or Web page; (b) when it reasonably appears necessary to do so to protect the integrity, security, or functionality of the College's computing resources or to protect the College from liability; (c) when there is reasonable cause to believe that the user has or is violating this policy; (d) when an account appears engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns; or (e) it is otherwise required or permitted by law. Any such individual monitoring other than that authorized by the user must be authorized in advance by the District Director of Information Technology.

C. The College may, in its discretion, disclose the results of any such individual or general monitoring, including the contents and records of individual communications, to appropriate College or law enforcement personnel, subject to the Family and Educational Rights and Privacy Act (20 U.S.C. §1232(6) and other applicable laws.

Subject to the exceptions set out above, users have reason to expect the same level of privacy in personal files on the College's computers (e.g., files in a user's home directory) as users have in any other space assigned to them by the College (e.g., a locker or an office).

Other organizations operating computing and network facilities that are reachable via the College network may have their own policies governing the use of those resources. When accessing remote resources from College facilities, users are responsible for obeying both the policies set forth in this document and the policies of the other organizations.

V. Enforcement

Users who violate this policy may be denied access to the College's computing resources and infrastructure, and may be subject to other disciplinary action or penalties both within and outside the College. Violations will normally be handled through the usual disciplinary procedures applicable to the particular user (i.e. faculty, administrator, staff or student) concerned. However, the College may temporarily suspend of block access to the College's computing resources or infrastructure prior to the initiation or completion of such procedures, when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of the College's or other computing resources.

VI. Designation of Agent for Notification of Infringement

In accordance with the Online Copyright Infringement Liability Limitation Act (17 U.S.C. 512), the District Director of Technology Services is designated as the College's agent for the receipt of any notices concerning any alleged copyright infringements occurring by reason of material being stored, transmitted, routed, or connected through the College's computing resources or infrastructure.