College Operating Procedures (COP)	FLORIDA SOUTHWESTERN STATE COLLEGE

Procedure Title:	Technology Acceptable Use
Procedure Number:	02-0405
Originating Department:	Office of Information Technology

Specific Authority:

Board Policy	N/A
Florida Statute	1001.65
Florida Administrative	N/A

Procedure Actions: Adopted: 6/9/2009; 6/01/2010; 7/24/2012; 04/29/2019

Purpose Statements To describe the limitations and practices that a user of Florida SouthWestern State College (College) IT resources must agree to as a condition of making use of College IT resources.

Guidelines:

As part of its educational mission, the College acquires, develops, and maintains computers, computer systems and networks. These Information Technology (IT) resources are intended for College-related purposes, including direct and indirect support of the College's instruction, research and service missions; College administrative functions; student and campus life activities; and the free exchange of ideas within the College community and among the College community and the wider local, national, and world communities.

This policy applies to all users of College IT resources, whether the users are affiliated with the College or not, and to all uses of those resources, whether on campus or from remote locations. Users are encouraged to periodically review the policy.

General Rules

Users of College IT resources must comply with federal and state laws, College Policies and College Operating Procedures, and the terms of applicable contracts including software licenses while using College IT resources. Examples of applicable laws, rules and policies include but are not limited to the laws of libel, privacy, copyright, trademark, obscenity and child pornography; the Florida Computer Crimes Act, the Family Educational Rights and Privacy Act (FERPA), the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act, which prohibit "hacking," "cracking" and similar activities; the College's Student Code of Conduct; the College's Sexual Harassment Policy; the College's Policy and College Operating Procedures on the Use of the College Name and Logos and the College's E-mail Policy. Users who engage in electronic communications with persons in other states or countries or on other systems or networks may also be subject to the laws of those jurisdictions and the rules and policies of those other systems and networks. Users with questions as to how the various laws, rules and regulations may apply to a particular use of College computing resources should contact the Information Technology Office for more information.

Users are responsible for ascertaining what authorizations are necessary and for obtaining them before using College IT 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 account administrator. 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 appropriate account administrator, the Information Technology Office, and/or Dean, Director, or Department Chair.

Disruptive use of College IT resources is not permitted. Units administering the resources involved will determine whether specific usage is considered normal, excessive or disruptive. Although there is no set bandwidth, disk space, CPU time, or other limit applicable to all uses of College IT resources, the College may require users of those resources to limit or refrain from specific uses if such use interferes with the efficient operations of the system.

Users may not use IT resources to gain unauthorized access to remote computers or to impair or damage the operations of College computers or networks, terminals or peripherals. This includes blocking communication lines, intercepting or sniffing communications, and running, installing or sharing virus programs. Deliberate attempts to circumvent data protection or other security measures are prohibited.

Users who violate this policy may be denied access to College IT resources. The College may suspend, block or restrict access to an account when it appears necessary to do so:

a) to protect the integrity, security, or functionality of College or other IT resources;
b) to comply with legal or contractual requirements;
c) to investigate alleged or potential violations of law or policy including, without limitation, state, federal, or local law, or College or Board of Trustees rules, regulations, policies, or collective bargaining agreements;
d) to investigate any asserted, threatened or potential complaint or grievance filed or credibly alleged pursuant to law or College or Board of Governors rules, regulations, policies, or collective bargaining agreements, or subject of law enforcement review or investigation;
e) or to protect the College from liability or disruption. The College may also refer suspected violations of law to appropriate law enforcement agencies for further investigation or action.

Users who violate the Policy may be subject to other penalties and disciplinary action, including expulsion or dismissal, under applicable College or Board of Trustees rules, regulations, policies, or collective bargaining agreement.

Security, Privacy, and Public Records

The College employs various measures to protect the security of its IT resources and user accounts. However, the College cannot guarantee complete security and confidentiality. It is the responsibility of users to practice “safe computing” by establishing appropriate access restrictions for their accounts, by guarding their passwords, and by changing them regularly.

College employees have access to sensitive College information which may include, but is not limited to:

- Financial aid information
- Personally identifiable information (PII) of students and employees
- Passwords granting access to College infrastructure and other programs
- Any other sensitive College information

Passwords should never be shared. The methods of storage and transmittal of sensitive College information internally or externally shall be by means approved by IT. Sensitive College information may be shared internally only with College employees who are authorized to receive such information. Outside vendors may only receive sensitive College information after they have signed a non-disclosure agreement and only by a secured means which has been approved by IT.

Users should also be aware that their use of College IT resources is not private. While the College does not routinely monitor individual usage of its IT resources, the normal operation and maintenance of the College's IT resources require the backup and caching of data and communications, the logging of activity, monitoring of general usage patterns and other activities necessary or convenient for the provision of service.

The College may monitor IT resources and retrieve communications and other records of specific users of IT resources, including individual login sessions and the content of individual communications, without notice.

Communications made by means of College IT resources are also generally subject to the Florida Public Records Law to the same extent as they would be if made on paper. In this regard, College personnel and agents should be aware that most written communications concerning College matters, regardless of whether College computing resources are used, are public records, many of which may be disclosed to the public upon request. Public records requests must be referred to the Public Information Officer or the General Counsel's Office for coordinating the response and review of requirements and exemptions.

Retention periods must be followed for all College records and communications as required by the Florida Public Records Law and any other applicable law or contractual requirements.

Commercial Use

IT resources are not to be used for personal commercial purposes or for personal financial or other gain. Occasional personal use of College IT resources for other purposes is permitted when it does not consume a significant amount of those resources, does not interfere with the performance of the user's job or other College responsibilities, and is otherwise in compliance with this and other College policies, including without limitation the College's policies on outside activities and use of College trademarks and names. Further limits may be imposed upon personal use in accordance with normal supervisory procedures concerning the use of College equipment.

Network Infrastructure/Routing and Wireless Media

Users must not implement their own network within the College’s infrastructure. This includes, but is not limited to basic network devices such as hubs, switches, routers, network firewalls, and wireless access points. Users must not offer alternate methods of access to IT resources such as modems and virtual private networks (VPNs). Users must not offer network infrastructure services such as DHCP and DNS.

Wireless is shared media and easily intercepted by a third party. Wireless users are encouraged to use some type of encryption. Users are also encouraged to password protect all individually owned devices that may contain College information such as emails and documents.