PROCEDURE

Subject	**Computer Hardware, Software, Security, Access and Electronic Communications**	**Number:** 2.60.01
Source	Human Resources	**Reference (Rule #)** 6HX14-
President's Approval/Date: 7-1-09		

PURPOSE: To provide State College of Florida, Manatee – Sarasota employees a policy for the appropriate use of College computer resources.

POLICY: Computer hardware, software, and access to Electronic Communications (E-mail, Voice Mail, Internet, and SCF Website) are College property, and thus use of these resources is subject to the rules and procedures established by the College.

I. INTRODUCTION:

The College provides a wide variety of computing and network resources for students and employees, that are intended for the legitimate business of the College.

Appropriate use of information resources includes instruction, research, and the official work of the offices, departments, recognized student and campus organizations, and other agencies of the College. Since the resources of SCF are not unlimited, the College may give priority for resources to certain uses or certain groups of users in support of its mission. Consistent with the College's anti-discrimination policy, the use of information resources should not be denied or abridged because of race, sex, religion, national origin, age disability, sexual orientation or marital status.

The following standards are established to provide access to the College's information technology resources to meet education and job related needs of students and employees, while maintaining the security and integrity of data files, and assuring the legal and ethical use of the software.

II. STANDARDS

A. General

1. Campus and network computing resources must be used in a manner consistent with Chapter 815, Florida Statutes Computer Crimes Act, Title 18, United States Code, Electronic Communications Privacy Act of 1985, and Public Records Law, Chapter 119, Florida Statutes and Chapter 286, Florida Statutes, the Government-in-the-Sunshine Law, and Educational Fair Use Guidelines for the Copyright Act of 1976 (Section 107), as amended and codified in title 17 of the U.S.C.

   Unauthorized or fraudulent use of the College's computing resources may result in felony. Prosecution and punishment as provided for in Florida Statutes, Chapter 775, Florida Criminal Code may be enforced.

2. The computing and network resources of the College may not be used for personal financial gain or commercial activity.

B. Hardware and Software:

1. SCF provides hardware and software, as required for the employees particular job functions, to be used for the sole benefit of SCF. Therefore, SCF shall have sole rights to the software and data used and/or stored on such computer equipment. The employee shall nave no claims to such hardware, software and data. Upon the employee's termination from SCF, SCF shall have no obligation to provide the employee with copies of any software or data stored on the computer equipment.

2. No unauthorized software may be loaded on SCF computer equipment and no unauthorized computer equipment may be used at SCF's facilities.

C. Internet/Electronic Mail

1. Access to the Internet and e-mail is College property and is, thus, subject to all requirements regarding use of College property or equipment.

2. Use of the Internet and e-mail is subject to the Public Records Law (Chapter 119, F.S.) and the Government-in-the-Sunshine Law (Chapter 286, F.S.).

3. Appropriate Use:

a. Internet

The Internet is to be used for accomplishing or enhancing the official business of the College by enabling the efficient and timely exchange of information and data. The Internet will be made available to staff, based on professional need as determined by Vice Presidents or their designees. Use of the Internet shall be guided by common sense and professionalism.

b. E-mail

E-mail is provided to staff to facilitate communication of official College business and to better fulfill the mission of the College. It includes functions such as electronic bulletin boards, information databases, and the ability to forward mail and route documents. E-mail shall be used for official College business and staff morale-building activities.

2) A copy of all messages transmitted and received via e-mail are subject to compliance with the Public Records Law (Chapter119, F.S.). Staff is advised to state nothing in an e-mail message that would be inappropriate if published in the news media. All e-mail may be saved on the archive server and subject to audit.

3) No aliases are allowed. All e-mail messages shall be credited to the actual author. All College employees using e-mail shall be assigned a unique electronic mailbox, accessible by an employee controlled password. No employee shall use another employee's electronic mailbox or password without permission from that employee.

4) No e-mail messages shall be transmitted or stored in encrypted form, unless approved by SCF management.

5) See SCF E-mail Guidelines - Appendix A on page 6

D. Security

1. Information systems are defined as computer, communications, and networking resources of all types (inclusive of but not limited to: mainframes, minicomputers, servers, switching equipment, network equipment, personal computers (PC's) to include all related internal and peripheral equipment and systems such as scanners and printers, etc., telecommunications systems, e-mail systems and services, web services, and Internet services).

2. SCF reserves the right to implement appropriate security measures, including denying access to information systems technology to anyone who, in the opinion of the College administration, has misused College information systems technology, as necessary to preserve and maintain system and data integrity.

3. Computer users must observe and comply with federal, state, and local laws governing computer and information technology. The College prohibits theft or abuse of information systems resources, including but not limited to:

    a. Unauthorized entry into a file or system to use, read, or change the contents, or for any other purpose.
    b. Unauthorized transfer of a file.
    c. Unauthorized use of another individual's identification and password.
    d. Use of computing facilities or telecommunications resources to interfere with the work of a student, faculty member, employee, or administrator.
    e. Use of computing or telecommunications resources to access, send, store, or display obscene and abusive messages or materials.
    f. Use of computing or telecommunications resources to interfere with the normal operation of the College computing or telecommunications systems.
    g. Unauthorized duplication or use of software or proprietary programs in violation of software licensing agreements.
    h. Willful introduction of computer viruses or disruptive/destructive programs into the College's network, any personal computer, or other component of the information system.

4. Employees Responsibilities Concerning Security

    a. Employees should report to their immediate supervisor the appearance of mysterious mission files or login notices which might indicate that the employee's files or systems access has been used without his or her consent.
    b. An employee should never leave a workstation logged on and unattended.
    c. Students are not permitted to use employee workstations without authorized permission.
    d. Employees must never give system or site-related information to unauthorized persons. Information requests concerning passwords, access, systems design or configurations should immediately be referred to the system administrator; no information of this nature is to be given out by the user.
    e. Employees should not download and execute software that is not job related from the Internet without appropriate authorization and testing.
    f. Employees must not accept instructions to type system-configuration "commands" into a system without appropriate authorization.
    g. No e-mail messages should ever contain passwords or security related information.
    h. Employees' receipt of any threatening communication should be brought to the attention of his or her immediate supervisor, system administrator, and campus security.

Note: records transmitted via an e-mail system are public records, and are therefore open to public inspection under the access provision of Florida's Public Records Law. Retention requirements are based on an analysis of the value of the contents of information, not on the media upon which it is recorded.

E. Web Page

1. The College web page is an official publication of the College and as such, the College reserves the right to control published content and links. The College web page shall be subject to the same requirements as all other College publications, including but not limited to, the laws, rules, and regulations regarding copyright, license, and confidentiality of student and employee records.

2. The design and construction of the faculty web pages shall be supervised by the appropriate Vice Presidents, Associate Deans and Directors.

3. The Webmaster, under the auspices of the computer services department, shall have oversight of all SCF website products.

F. Licensing

Software is licensed to SCF for specific and restrictive use. Therefore, it is illegal to copy licensed software for personal use, either on campus or off campus. Appropriate authorization may be given to allow licensed software to be installed on an employee's home computer. Pre-approval is required.

G. Copyright

All federal Copyright laws as they relate to computer use shall be observed.

H. Inappropriate Use

Using these resources for purposes other than for the official business of the College is inappropriate and unacceptable use of the Internet or e-mail. Such inappropriate uses include, but are not limited to, the following:

a. Purposely seeking to gain unauthorized access to other computers, which is referred to as hacking.
b. Purposely disrupting the intended use of the Internet or e-mail.
c. Wasting College resources by undertaking activities that cause the employee to be continuously idle or non-productive during work hours. This includes, but is not limited to, wasting time, engaging in idle talk or gossip, game playing, excessive surfing (exploring), connecting to inappropriate non-work related addresses, or conducting personal business.

d. Purposely destroying the integrity of computer-based information (e.g. introducing viruses) or otherwise using College information resources property negligently or carelessly so as to place College information resources in such a position as to unreasonably increase the likelihood that it will be damaged, destroyed, or stolen. Information resources include hardware, software, and data.
e. Using the Internet or e-mail for illegal purposes, including but not limited to, copyright infringement, and downloading illegal software.
f. Knowingly submitting inaccurate or untruthful information for or on any College record, report, or document.
g. Making unwelcome sexual advances, requesting sexual favors, or any other conduct of a sexual nature. These actions may constitute sexual harassment and will not be tolerated.

h. Transferring material which is threatening, abusive, or obscene, or which creates an atmosphere or situation which detracts from the employee's ability to get along with other employees or supervisors or the general public, or which unreasonably reduces the employee's ability to effectively complete his or her job duties, regardless of intent.
i. Soliciting funds or services, selling tickets, or distributing petitions or literature for any purpose other than official College business.
j. Reading, deleting, copying, modifying or otherwise using any other employee's e-mail without his or her permission.
k. Charitable or commercial advertisements, other than official College business, or pre-authorized personal advertisements on the official employee "classified" page of the intranet, are prohibited.
l. Annoying other employees with excessive or irrelevant e-mail.

Inappropriate use of the Internet or e-mail or violations of this procedure shall be subject to disciplinary actions, which may result in a written reprimand, suspension, or dismissal.

SCF GUIDELINES FOR E-MAIL

The electronic mail system is a finite resource that is intended to facilitate and support our mission as a comprehensive community college. To maximize the effectiveness of this tool we suggest the following guidelines be followed:

1. It is impossible to insure the confidentiality of any electronic message stored or communicated through our computing facilities. Moreover, the courts have ruled that email is public record, so keep this in mind when you create and send any email.

2. Do not use e-mail for items that need immediate attention. It is best to call/visit the people who can help solve the problem.

3. In all messages, provide the reader with information about the e-mail content. Use a detailed subject/header to provide this information.

4. Before sending out an e-mail message to everyone on the network, or everyone on a distribution list, ask yourself if everyone needs this information. Copy only those people who are "stakeholders." Often, email messages are sent out to everyone because it's the easy thing to do.

5. Keep text brief and to the point, 1-2 small paragraphs or "bullets."

6. Use proper writing rules (e.g., start each sentence with a "Capital Letter"). However, do not use all CAPS for the entire message.

7. Do not use e-mail for analytical purposes (i.e., it is not usually the best mode to debate an issue, when a meeting or a phone call could bring closure to the matter at hand).

8. Realize that a message you send to someone may easily be forwarded to many other individuals, whether or not you had intended it for broad distribution. Proper etiquette is to ask permission before you forward an email to others.

9. Include greeting with specific name (so reader knows to whom the message is addressed).

10. Basic writing principles apply – write to your receiver's interest and level.

11. Remember! Your e-mail gives the reader an impression of the College (good or bad).