Technology Usage Acknowledgement

Before you are issued a User ID and Password to access the SFSC network, you must read this document in its entirety, sign this form, and forward it to the IT Department. Upon receipt of the signed form, the IT Department will issue you a User ID.

I have received, read, understand and will abide by the requirements set forth in the South Florida State College Technology Usage Guidelines and Support Manual. I will review the guidelines annually for any additions and updates. I understand that the use of technological resources at South Florida State College is a privilege as opposed to a right or entitlement. I also acknowledge that I will take all necessary steps to ensure the security and safety of the technological resources and data to which I may have access.

_____ _____

Employee Signature Date

_____ _____

Printed Name SFSC Employee ID (GID)

Revised: July 2012

S O U T H F L O R I D A
STATE C O L L E G E

Technology Usage Guidelines
And Support Manual

Revised July 2012

South Florida State College
Technology Usage Guidelines and Support Manual

Table of Contents

Information Technology Operational Guidelines

User Access and Privileges *1*
Hardware and Software *2*
Security *8*
Email *11*
Internet *12*
SFSC website, Panther Central Portal and Social Media *13*
Data Entry/Access *14*
Service Calls *15*
Telephone Support *16*

Academic Technology Support

Introduction *17*
IT Media Services *17*
eLearning Department *18*
Network Systems *19*

Security Awareness

Introduction *20*
Why is Information Security Awareness Necessary? *20*
How Secure Are You? *20*
Physical Security for Technology Resources *21*
Anti-Virus Software *21*
Outdated Operating System Software *22*
File and Folder Sharing *22*
Backing Up Data Files *23*
Welcome to the Internet *23*
Email Usage *24*
Password Protection *24*
Why Should I Worry if Someone Has My Password *25*
Privacy of Student and Employee Records *25*
Copyright or Copywrong? *26*

Appendix

Acceptable Use of Technology for SFSC Employees
Copyright and Licensing Agreements
Technology and Innovation Assessment Process
Social Media Guidelines

Definition of Terms

Access	1. Direct (or local) entry into the SFSC network using a computer or other input device 2. Remote entry using communication lines
Application System	Any software that, together, comprises an entire database maintenance system which includes data entry, reports, etc.
Client Application	A program or part of a program that resides and is run from the user's workstation
Network Application	Program or part of a program that resides and is run from the network server
Banner	SFSC's registration, student information, payroll, and etc. application system
Computer System	Any personal computer (PC), workstation, or server on or off the SFSC network
Drive	Storage area either on the local workstation or on a server (appears as a hard disk drive)
Drive Mapping	Assigning a letter (t:, u:, y:, etc.) to network applications or devices
IT	Information Technology Department
Loading (Software)	Installing software program(s) on a computer for use
Network	A number of connected computers that share information and devices
Network Drive	A drive that resides on a server computer rather than on the local computer
Panther Central	Intranet portal used to access information from Banner
Server	High capacity PC used to share programs and files
Workstation	Any personal computer (PC) used to access SFSC network
User	Any college employee, vendor, or contractor who has been permitted access to the SFSC network by his/her User ID and password
User Profile	A configuration for a specific user: rights, permissions, and privileges defined
Panther Den	Desire2Learn (D2L) course management system used for SFSC online classes

User Access and Privileges

New employee user access is granted after the signed acknowledgement, located at the beginning of this document, has to been returned to IT and Human Resources has notified IT that employment is verified and they have received all required paperwork.

For further clarification of any IT service, contact the Help Desk, and we will be glad to answer any questions you may have.

1.1 New Employee User Access

As a new employee you will be assigned a User ID by IT. The User ID is typically the first seven characters of your last name and the first character of your first name.

Example:	John Community	communij
	John Jones	jonesj

To avoid duplication of User IDs, there is a possibility that a User ID may deviate from the examples listed above.

It will be your responsibility to follow the IT guidelines in this manual when using your assigned User ID.

A temporary password will be given to all newly created User IDs which you will be required to change the first time you log onto the network.

Note: To access your Email through the Internet, you must first sign into the network on campus (for more information on Email see the section titled "Email").

As a new employee, you will be permitted to sign onto the SFSC network, use the Internet, use Email, and use the college portal, Panther Central. This basic access is given without a User Profile. For additional access, your supervisor will need to submit a User Profile: see Additional Rights later in this section.

1.2 Restrictions

Some restrictions are applied to the workstations and User IDs such as:

- Programs cannot be loaded without the assistance or prior approval of the IT department. This prevents conflicts with standard SFSC installed applications as well as copyright infringements. Rest assured, you will always have the access and privileges that you need to perform your job.

- No network changes or drive mappings (assigning drive letters to a network server or printer) are allowed without IT intervention. This prevents users from mapping drives that can conflict with the standard drive letters that the college uses to run various applications.

1.3 Additional Rights

If you need more privileges and access than what is given with basic access, such as access to department drives on the network, Banner, etc., your department head must fill out a "**User Profile**" form, which is located in the All Public Folders\Forms section in the Email system. The User Profile form is used to grant rights in the Banner system (view, edit, create information).

If you are granted additional rights, you will be given a home folder on the network (U: drive). This folder will be limited to a size of 50 MB. You may also be granted rights to the R: drive which is for temporary storage only. It can be used to share information with others. **Warning: this is a non-secure drive open to everyone. Information is not backed up by IT and can be deleted by anyone with access to the drive.**

If a user needs access to the imaging system (OTG), a request form must be completed and forwarded to the IT Department.

Faculty may also receive access to the Desire2Learn (D2L) learning management system. For more information, faculty should contact their department chair or the eLearning Department.

1.4 Access Hours

The network shall be available to college staff seven days a week, generally from 6 a.m. to 10 p.m. Panther Central self-service applications are available 4 a.m. to 10 p.m. The only exceptions to this would be when maintenance is required for the online servers. Normally, server backups and maintenance software shall run 8 p.m. to 6 a.m. Email will be available 6 a.m. to 10 p.m.

Hardware and Software

All hardware and software requests must be approved by IT before purchase. This included both purchase order and college purchasing card (P-Card) purchases.

All software, except for SFSC standards listed in section 2.1, must be evaluated and approved by IT. This includes free software packages, web-based software and software purchased with a purchase order or college purchase card (P-Card)

Our goal is to provide the highest quality service. When requesting service, please give IT adequate notice before the deadline; otherwise, we cannot guarantee that your request will be completed by your deadline. To plan appropriately, some services require advanced notice, such as ordering equipment, loading software, large departmental moves, physical changes involving wiring, etc. For your information, we have included a schedule guide on most services. See section 2.7 titled Schedule Guide.

2.1 SFSC Computer PC and Software Standards

Hardware

The IT Department establishes and maintains a standard configuration for computer equipment at SFSC. For a copy of the most recent standards information, please check in the "Computer Standards" document on the Employee tab in Panther Central, or contact the IT Help Desk at ext. 7462.

Software

SFSC has entered into a Campus Agreement with Microsoft for Windows and Microsoft Office. This agreement entitles SFSC to use the above products on all workstations without any unit cost. This software is considered the standard.

In addition to the above software, all SFSC PCs will have anti-virus, Banner, Adobe Reader, Flash Player, QuickTime Player, Real Player, and PrintKey software loaded on them.

Academic software, whether purchased or available free, must be verified by IT to be compatible with the college infrastructure, supportable with existing resources, and comply with college technology security policies.

2.2 Purchasing PC Equipment and Software

PC Equipment and Peripheral Requests

IT maintains a set of standards which have proven to work in the SFSC environment (see SFSC Computer PC Standards, above). A standard PC runs only the standard SFSC approved software.

> *SFSC Standard Configuration PC*: If you want to purchase a standard configuration PC from the posted list, submit a request to the IT Help Desk. IT will ensure the configuration/price has not changed.
>
> *Non-standard Configuration PC*: If you wish to purchase a PC that varies from the SFSC standard, please call the IT Help Desk at ext. 7462 or Email (just type "Help Desk" in the TO field) for assistance. An IT employee will be assigned to respond to your request. You should complete the Request for Software and Hardware Assessment (RSHA) to ensure all computer equipment is compatible with the college infrastructure. See section 2.8 in this document.
>
> *Peripherals/Upgrades*: To order peripherals or upgrades, the department head should submit a letter or Email of explanation to IT Help Desk explaining why the peripherals or upgrades are needed. The following information should be included in the letter of explanation:
>
> - Name of employee(s) receiving equipment.

- The SFSC property number of equipment which is being added to or upgraded.
- A proposed timeframe.

To avoid a processing delay for all purchases, include the:

- Quantity and description of the item(s)
- Name of receiving employee(s) and their department(s)
- Proposed location of the new PC
- Approval signatures

These requirements are needed to allow IT to schedule installation, check for network connections, check for power outlets, etc.

Software Requests

Most software has a copyright notice and a license agreement. SFSC must comply with both of these. Since there can be several penalties for breaking copyright procedures or license agreements, read and understand them for each piece of software you use. You should also read and understand the copyright and licensing information listed in the appendix of this document.

IT installs the software listed in section 2.1 in all new workstations and whenever a workstation is reassigned or reloaded. If any workstation does not have the standard products and any of them are needed, please contact the IT Help Desk at ext. 7462 or send an Email.

Academic software, whether purchased or available free, must be evaluated to determine compatibility with the college infrastructure, supportability with existing resources, and compliance with college technology security policies. Software being considered for a new course or a significant change to existing course software must go through the academic approval process outlined in the academic support section of the *eLearning Handbook*

Before ordering software other than the SFSC standard software, please contact the IT Help Desk at ext. 7462 for assistance. You should complete the **Request for Software or Hardware Assessment** (RSHA) form (located in the appendix and on the Employee tab in Panther Central). See Section 2.8 of this document for more information.

Purchasing Process

IT will initiate a work order for the evaluation/price quote/purchase requisition.

Upon completion of the above request process, IT will send a completed purchase requisition the requestor. Upon receipt of the purchase requisition, please have the accounting codes and appropriate signatures entered on the purchase requisition. Send the purchase requisition to the Purchasing Department for processing.

2.3 Receiving PC Equipment and Software

Unless previously arranged and approved, **all computer equipment and software must be received and distributed by IT**. This is to ensure the timely receipt of all incoming computer items, as well as verification that the merchandise we received is what was ordered. Once the equipment or software is received in IT, we will validate the internal/external components for accuracy and coordinate the necessary action (if any) needed for installation and/or training.

Software Installation

All software must be installed with the assistance of the IT Department. Software that will be installed on SFSC equipment must be licensed to SFSC, be legal meeting all license and copyright guidelines, and be consistent with the educational mission and goals of SFSC. Software must also be compatible with the SFSC network environment. To have software installed, call or Email the Help Desk to initiate a service request. Please have the following information ready:

- Title of software.
- Version.
- SFSC property number of the computer the software will be loaded on.
- Is it a network or client application?
- Minimum computer requirements.
- Location of computer on which software will be installed.

2.4 Moving PC Equipment and Software

PC Equipment

Under no circumstances should an SFSC computer be disconnected from the network or moved to another location without direct assistance from IT. We will attempt to meet your moving request(s) in the time frame that you stipulate. However, for us to comply with your requests, we will expect adequate notice **prior** to moving the equipment. Simply follow the steps below for all PC moving requests.

- See *Schedule Guide* section 2.7 for appropriate time frame of notice needed.
- Notify the Help Desk (in writing or Email) of the upcoming move.
- List all details, include employee's name and phone extension(s) (from and to).
- Include equipment (workstations, printers, scanners, etc), place of origin, and where the equipment is to be moved.
- Include a diagram if possible. Be sure to include phone moves, and any other changes or additions in wiring (phone or PC).
- If you have questions, contact the Help Desk at ext. 7462 or via Email.

Software

Under no circumstances should software be removed from or installed onto a workstation without direct assistance from IT. We will try to abide with your moving requests and meet your office needs in a timely manner. However, for us to comply with those requests we need adequate notice. Some software cannot be moved to another computer by law. Simply follow the steps below for all software moving requests.

- Contact the Help Desk at ext. 7462 or send an Email.
- Include the SFSC property number of the equipment and its location.
- Include the title and version of software to be moved.
- If you have questions contact the Help Desk at ext. 7462 or send an Email.

2.5 Re-assigning PC Equipment

Under no circumstances should an employee move or re-assign any SFSC computer equipment to another location without the direct supervision from IT. To maintain accurate records, we need to be advised when you want such equipment reassigned. Let us know what has to be moved or re-assigned as early as possible.

Initiate a service request. Include the location, the user, the hardware, and the software involved. This can be done over the phone and then followed up with an Email request which should be submitted to the IT Help Desk. We will notify the property manager of the change. The property manager keeps track of where all SFSC machines are within the college. Please note that any loaded software stays with the original machine unless the user requests the software to be transferred also. In a typical re-assignment, IT will reformat the hard drive before reassigning the equipment.

2.6 Non-SFSC Equipment and Software

Any connection of non-SFSC Equipment to the SFSC network or stand-alone computers is prohibited. The use or installation of non-SFSC owned or licensed software is prohibited. If special circumstances exist, please contact the IT Help Desk.

2.7 Schedule Guide

Type of Service	Minimum Lead Time	Comments
Moving Equipment	1 week – 2 weeks Depending on number of PC's or preparation, *IT* may need up to 1 month for cabling and preparation.	Note: User must coordinate with the Maintenance and *IT* Departments to give as much notice as possible.
Installing Software	As much notice as possible. Depending on number of PC's or preparation, *IT* may need up to 1 month.	*IT* may have to contact the software vendor to configure the installation for the SFSC network and to meet user requests.
Requesting User Profiles	3 business days	Department heads will need to submit a form indicating the desired access for the employee.
Network Cabling	2 weeks - 1 month Call *IT* as soon as any move or new project is planned.	New Cabling **Note: Coordinate with *IT* when you are in the early planning stage**, definitely before any vendor commitments have been finalized. The requesting department will be responsible for the cost of the cabling.
Service Calls	Serviced in the order in which calls are received (student equipment has first priority).	
Application Programming	Requests will be evaluated and decision made as to the length of time required.	
New Equipment	Within 2 weeks after receipt of equipment from vendor.	
Requested portal enhancements/changes	Within 5 business days after approval by Portal Advisory Committee	
Academic Technology Resources Evaluation	1 week – 2 months depending on the complexity of testing.	May require a meeting with the Technology Resource Review team (see academic support section of this document).

The above schedule will be followed whenever possible. There may be unusual times throughout the year where exceptions might occur.

2.8 Request for Software or Hardware Assessment (RSHA)
(Includes free software and Internet resources)

Academic software, whether purchased or available free, must be evaluated to determine compatibility with the college infrastructure, supportability with existing resources, and compliance with college technology security policies. Software being considered for a new course or a significant change to existing course software must go through the academic approval process outlined in the academic support section of the *eLearning Handbook.*

The definition of hardware, technology, and innovation can be found in the **Technology and Innovation Assessment process** document located in the Appendix and on the Employee tab in Panther Central.

Before ordering software or hardware other than the SFSC standard, please contact the IT Help Desk at ext. 7462 for assistance.

You should complete the **Request for Software or Hardware Assessment** (RSHA) form (located in the Appendix and on the Employee tab in Panther Central). The request will be reviewed by the CIO. If approved for consideration, an IT employee will be assigned to your request to test the software/hardware for compatibility in our environment. Once certified, IT will approve the purchase. To avoid delay follow the **Technology and Innovation Assessment Process** (located in the Appendix and on the Employee tab in Panther Central). The approved process is as follows:

- Allow sufficient lead time for IT to plan the installation or configuration of existing software and/or devices.
- Follow the steps in the Technology and Innovation Assessment Process: 1) consult with department head/dean; 2) submit a RSHA to IT for evaluation; 3) IT will determine compatibility in our environment. 4) If certified, IT will approve the purchase.
- Once approved, IT will forward a purchase requisition (quote is only good for 30 days) to the originator.
- If purchasing with a college purchase card (P-Card) the originator must obtain an IT staff signature on the price quote to verify IT approval. It is highly recommended that purchase orders be used for purchases.
- Originator will forward the purchase requisition to Purchasing.
- Purchasing department will complete the purchase transaction with the vendor.
- IT will install the software/hardware when it arrives (includes internet software downloads).

Security

3.1 General IT Security

To prevent data corruption, theft, or modification, we expect every SFSC user to do the following:

- Protect your password.

- Store your computer's documentation in a safe place.
- Store your software in a safe and secure place.
- Log out when leaving a computer.
- Never log in to more than one computer at any given time.
- Always backup your data (if a user needs help or instructions on how to do this, he/she should contact the Help Desk).

If you feel you have received a virus, shut off your computer **immediately** and call the Help Desk. If the computer is not shut off, you might spread the virus across the SFSC network. A technician will be dispatched to check your computer immediately! Usually the anti-virus software will display a message notifying the user of a possible virus.

3.2 Physical Security

Physical security is the first step in keeping data and your computer secure. When leaving your office, secure the door unless your office is in a secured area. Students and/or guests should not be left unsupervised in an area where there are computers.

When using a laptop computer outside the office, be conscious not to leave it unattended. Remember, confidential information could be stored on the drive.

Only authorized users will be permitted access to the IT computer room. This is an audit requirement that must be followed.

IT reference materials (i.e. system manuals) shall not be removed from the computer room except by IT personnel. If removed by authorized staff, these reference materials will remain in their possession until they return the reference materials to the computer room.

3.3 Passwords

Your password is your key to unlock your access to the network, Email, and student data. **Protect it. Do not give your password to anyone**. If there is a breach of security, notify IT immediately. Your network and Email password must be changed every 60 days. You cannot reuse the last six passwords. You may have additional passwords besides the ones mentioned above. You should protect these passwords as well. Disclosure of your password will constitute a security breach and may, if considered serious enough, subject the employee to disciplinary action.

IT does not have the capability to view passwords. If you forget your password, you must call the Help Desk to have your password reset.

For more information see "password protection" in the "Security Awareness" section of this document.

3.4 Network Security

The SFSC network is used to share information among all of its campuses. To keep the network secure, please do the following:

- Use a password on your screensaver (contact the Help Desk if you need assistance with this security measure).
- Never give anyone your password.
- Use difficult passwords. Don't use names or common words. Try to include alpha-numeric and special characters.
- Never let someone other than IT work on a computer that you are logged on to.
- Log out if you are leaving your area.

The communications jacks are monitored and configured for a specific workstation. Do not plug any personal or previously unused devices into the network without consulting IT before doing so.

SFSC also has a Guest wireless network which provides internet access for visitors' personal laptops and other mobile devices. The guest network access is a courtesy for the community which is not guaranteed dependable and should not be considered an academic resource.

3.5 Computer Room and Server Security

No individual other than authorized IT staff members will be allowed in the computer room without expressed consent of the CIO and direct supervision by an IT staff member. All visitors are required to sign in before entering.

No user, IT staff member, or other person shall be signed on to the system console unless they are using it. If not in use, the system console will be signed off. All servers will reside in the IT computer room.

3.6 Security Rules Concerning Student and Class Records

The college has specific policies and procedures in place to protect the confidentiality and privacy of Student Records. South Florida State CollegeProcedure 2152 deals directly with the Family Educational Rights and Privacy Act (FERPA).

You are required, as a college representative, to abide by these laws, policies, and procedures. You should review the South Florida State CollegeManual of Policy and Procedures. SFSC Policies and Procedures are located in the POD tab of Panther Central. All employees have access to the POD tab.

Email

4.1 Appropriate Use

The SFSC Email system is first and foremost for business purposes; thus, its primary use should be to exchange information that is relative to the college's business. Using it for personal Email should be limited.

You should never initiate inappropriate mail. Your Email should consist of appropriate topics and language that would appear in a formal memorandum or a telephone conversation.

Florida's Public Records Law requires that all Email used to make business decisions must be saved. Email is public information and it has to be accessible upon request. This is your responsibility to save this vital information. More detailed information is available in the Appendix under "Acceptable Use of Technology for SFSC Employees". If help is needed, please call or Email the Help Desk.

Email offers many opportunities for security problems. Email can easily be forged and does not necessarily afford the privacy one might expect. Here are some things to keep in mind when using Email.

- The name on an Email message is about as useful as the return address on an envelope. It can easily be forged by a virus or individual. Keep this in mind when you take action based on Email messages. In particular, be cautious about opening attachments, giving out personal information, or altering your computer based on information in the message.

- Don't give out confidential information in response to an Email. For example, someone may try and persuade you to give out your password or a credit card number. You may not know whom you are dealing with. No reputable organization will send you an unsolicited Email message with a program like a patch or software update as an attachment. They will always reference an official website where you can download it. Before doing so, make sure it is an official website and not something that just looks like one. If you are not sure, contact IT.

- Be wary of unsolicited technical advice. Strangers may suggest certain things that could easily expose your computer to another environment.

- Be wary of mail attachments that you don't know anything about. This also applies to Web downloads. It's very easy for a computer virus to be present in Email from people you know and people you don't know. **Although the college uses anti-virus software that checks all Email, new viruses are created at an alarming rate, and there is no guarantee that the anti-virus software will catch all of them.**

- If you receive abusive Email, it should be reported to your supervisor so action can be taken. It is suggested you do not delete the message, as it can often be useful in tracking down the incident.

As has been stated before, don't share your Email password or keep it written down where it can be easily discovered.

4.2 Email Address

The SFSC domain is "southflorida.edu." As an employee of SFSC you have several Email aliases with which you can receive Email (example aliases@southflorida.edu). The aliases are listed below (John Observer is used as an example name):

Last name + first initial	observerj@southflorida.edu
First seven letters of last name + first initial	observej@southflorida.edu
First name.last name	john.observer@southflorida.edu

4.3 Storage

Every SFSC employee is allocated ample Email storage in their Email inbox.

One way to prevent using more than the allotted storage space is to save or archive your Email in a personal folder. These folders are stored on your local drive and not the Email server. As always, you can receive help with this procedure by calling the IT Help Desk at ext. 7462 or sending an Email. Remember to backup Email archives regularly.

SFSC automatically archives all Emails. This process occurs before any recipient receives his/her Email. Also, all outgoing Emails is archived. This archive process has been implemented to comply with state and federal compliancy rules and regulations. It is **not** a typical backup/restore process from which IT can restore an accidently deleted Email.

Internet

5.1 Appropriate Use

All employees have access to the Internet from the college. This access should be used in a responsible, efficient, ethical and legal manner.

Under no circumstances should you enter your SFSC User ID and password on any website other than a SFSC website or page. If you do not adhere to this, you could jeopardize the security of your user login.

Try not to use your SFSC Email address as a User ID. Using your Email address can cause you to receive SPAM.

For more information on use of the Internet, please see the "Welcome to the Internet" topic of the Security Awareness section of this document

5.2 Restrictions

There are specific restrictions regarding Internet use. Please refer to the "Acceptable Use of Technology for SFSC Employees" in the appendix of this manual and on the Employee Tab in Panther Central.

SFSC Website, Panther Central Portal and Social Media

6.1 Appropriate Use

Content within the SFSC website and portal may be created for academic departments, administrative departments, college-sanctioned organizations or committees, employees, and official student organizations.

Publication of any material on SFSC's website and portal must be consistent with the policies, regulations, standards, and procedures of the college and the Acceptable Use of Technology for Administrative, Faculty, and Staff Use, as well as applicable state and federal laws.

SFSC reserves the right to control college resources, including but not limited to denying space on college-supported servers or removing any links to content that it perceives as not upholding the rules, policies, standards, and procedures of the college as well as applicable state and federal laws. Editors of information over the campus network shall accept full editorial responsibility for their content and documents.

Social media are w
eb-based tools, also known as cloud computing, that can provide immediate publication of content to the Web and enable interaction between the person posting the message and her/his audience. Examples are blogs (Blogger, WordPress), micro-blogs (Twitter), social networking sites (LinkedIn, Facebook, MySpace, Google+), wikis (Wikipedia), photo sharing sites (Flickr, Picasa), and video sharing sites (YouTube).

SFSC has social media guidelines for SFSC faculty, staff, and administrators; students acting as official SFSC representatives; and contractors creating or contributing both on and off www.southflorida.edu. Before using any social media resources for college related purposes, employees and students should review the Social Media Guidelines and submit a completed request form to Community Relation (posted on Panther Central under Public Relations Resources.) The guidelines can be found in the appendix of this document and in Panther Central.

Academic freedom in teaching and the right of freedom of speech for employees and students are fundamental principles of the college. SFSC Web and portal publishing policies and regulations do not limit or remove the right of free speech. Although SFSC believes that the principles of free speech and academic freedom extend to electronic

communication, the college is not obligated to publish information or provide links to documents or external content that are deemed to be inappropriate.

Reasons that content, documents, or linked pages might be deemed inappropriate for display on the Web or portal include but are not limited to the following: publishing copyrighted or trademarked materials without written authorization, violating elements of the Family Educational Rights and Privacy Act (FERPA), receiving compensation for providing material to any party not entitled to use college resources, publishing organized political activities, opinions or solicitations, selling or buying products for profit enterprises, and incorporating advertising for promotion of non-profit or for-profit entities.

In general, college policies and regulations that apply to the content of publications and communications also apply to Web and portal content published using SFSC's Web servers. In particular, all information included in Web pages on SFSC Web servers must:

- Comply with all laws governing copyrights, intellectual property, libel, and privacy;
- Not violate any policy, rule, or regulation of the college;
- Not be used for non-SFSC commercial activities (for the purposes of this regulation, activities such as publishing textbooks and other academic works are considered to be SFSC activities); and
- Comply with SFSC policies, rules and regulations.

6.2 Restrictions

Any person who uses the SFSC Web and portal resources consents to all of the provisions of this regulation and agrees to comply with all of its terms and conditions and with all applicable local, state, and federal laws and regulations, and Acceptable Use Policy. Please refer to the "Acceptable Use of Technology for SFSC Employees" in the appendix of this manual and on the Employee Tab in Panther Central.

Data Entry/Access

7.1 Appropriate Use

Entry of data shall be performed by the department member responsible for the application system information. The dean/director will assign the responsibility for data entry within their division/department, at his or her discretion.

Access to data, whether for update or inquiry, shall be coordinated between the responsible dean/director and IT. Access to data shall be granted to an employee only when it is required for their position responsibilities.

To prevent unauthorized access, it is your responsibility to log off of your workstation when it is not in use or when you are away from your workstation. Numerous infractions of this policy may lead to a user having their User ID and password revoked.

You must not reveal your password to any other college employee. You should not sign onto a workstation so that another college employee may gain access to the SFSC Network. Any event of this nature is a breach of security and can lead to having your User ID revoked and may result in disciplinary action.

Under no circumstances shall any person(s) or agency outside of the college be given access, either on-site or off-site, to computer software, files, or hardware without the express consent of the CIO or the college president. This includes, but is not limited to:

- Software/files contained on the SFSC network
- Software/files contained on diskette (or other storage media)
- Program or file listings
- Printed reports, by an application system, contained on hardcopy
- Files stored on Email

Service Calls

8.1 Placing a Service Call

To place a service call, please call ext. 7462 or Email the Help Desk with your request. You will be required to furnish your name, telephone number, location, SFSC property number, and the nature of the problem.

In most cases you will receive a call from the IT technician assigned to your work order within two hours. The technician will then confirm your request and he/she will schedule a date/time of repair.

Service calls are taken in the order of receipt, except when there is an emergency. Classroom and computer lab equipment have first priority.

8.2 Hours of Service

Normal office hours are Monday – Friday, 8 a.m. – 5 p.m. IT is available as "best effort" for emergencies at all other times. In the event of a long term power failure, please notify security.

Evening/Weekend Service

After hours service is for emergencies of scheduled classes and events only.

If emergency service is needed for technologies on the weekend or during the evening, please call SFSC Security at 453-0806. The SFSC Security team will notify the

appropriate technician. Evening service is available Monday – Thursday, 5 p.m. – 7 p.m. Saturday service is available 8 a.m. – 4 p.m. There is no guaranteed response time.

Service is available for the following technologies:

- Computer hardware
- Network
- Email
- Internet
- Computer software systems (Banner, etc.)
- Media equipment (projectors, smart podiums, document cameras)
- Telephones

Telephone Support

The college telephones should be used primarily to conduct SFSC business.

9.1 Tri-County Area (Highlands, Hardee, and Desoto)

To complete a telephone call within the tri-county area dial 9, then the telephone number. The telephone switch will automatically route the call.

9.2 Calling Long Distance

Employee telephones have long distance access, while student telephones do not.

To complete a long distance call dial 8, then 1, the area code, and then the telephone number. Whenever possible please use a toll free number.

To complete a toll free call, dial 9, then 1, the area code, and then the telephone number.

9.3 Repairs

To place a repair call, please call ext. 7462 or Email the Help Desk (helpdesk) with your request. You will be required to furnish your name, telephone number, location, and the problem.

Telephones repair calls are considered the same as service calls. See Service Call section of this document for information on the service call process.

9.5 Installation and Changes

To have a telephone installed complete the **User Profile** request. Forward the completed form to IT. This form must be approved by your dean or director.

Contact the IT helpdesk for telephone option changes.

Introduction

This section is dedicated identifying the responsibilities and resources of the departments that provide academic technology support for the college.

Academic software and other technology resources, whether purchased or available free, must be verified by IT to be compatible with the college infrastructure, supportable with existing resources, and comply with college technology security policies. Please refer to the Request for Software and Hardware Assessment section 2.8 of this document and the *eLearning Handbook* for information regarding academic technology guidelines.

Media Support and Network Systems are a part of the Information Technology Department and reports to the CIO. Media Support provides technical support and training for classroom technology and assistance with video, teleconferencing, and Web conferencing. Network Systems provides technical support for the two-way interactive system in addition to the resources mentioned in previous sections.

The eLearning Department, which reports to the vice president for educational and student services, provides support for the Desire2Learn (D2L) learning management system, faculty and staff technology training, support for academic software, support for eLearning courses, and multimedia support and development.

The IT and eLearning departments are part of a Technology Resource Review team which assists during the course development process, when possible course resources are planned. The team, which may also include additional technology savvy college employees, will meet with the instructor to review and discuss any technologies planned for the course and to receive additional resource ideas and support.

IT Media Support

1. Classroom Support

IT media support staff provides planning, technical support for smart classrooms and other media needs for the campuses located in Highlands, Desoto, and Hardee counties. The college has smart classrooms and smart labs. Classroom support includes:

1. Troubleshooting of podium technical components
2. Training on the use of podium – faculty must be trained before receiving a key to the podium
3. Assistance with presentations (insuring that presentation can be viewed from CD, DVD, computer, or USB device)
4. Media cart support for classrooms without permanent media technology

All employees that use smart classrooms must be trained by IT media support staff on the use of the smart podiums. Full-time and adjunct faculty may receive a key to the podium upon completion of training.

2. Media Equipment

IT media support staff is responsible for the research, selection, and support of appropriate instructional media technology to enhance the learning environment. The responsibilities include:

1. Assisting in the design and selection of instructional facility media technology
2. Overseeing installation and implementation of media equipment by vendors
3. Supervising repair and maintenance of media equipment
4. Maintaining an inventory of media equipment available for short-term or long-term loan to faculty and staff

3. Hours of Service

See Hours of Service Section 8.2 of this document.

eLearning Department

This section is dedicated to academic resources provided by the eLearning Department. Contact the eLearning Department for more detailed information on services and support.

1. User Support

The eLearning staff is available to provide user support for the academic technology available for use at SFSC. In addition, they provide Microsoft Office training for faculty and staff. The eLearning staff provides academic support for:

1. Instructional applications and technologies
2. Video production, editing, and duplication
3. Multimedia presentation and resource production (instructional and non-instructional)
4. Research and selection (with assistance from IT) of new and appropriate technologies for instructional purposes
5. Regular technology training classes
6. Educational software applications and information (Skills Tutor, Derive, etc.)
7. Instructional Resources Management-Accessibility/Compliance with the Americans with Disabilities Act (ADA)
8. SFSC copyright policy
9. New employee training

2. Online Learning Support

The eLearning staff is available to provide support for the Desire2Learn (D2L) learning management system and other online learning assistance. The eLearning staff provides academic support for:

1. D2L learning management system support and administration
2. eLearning courses - coordination, instructional design and management
3. eLearning quality evaluation

4. Development and administration of The Orange Grove – Learning Object Repository (LOR)
5. Satellite system administration
6. Panther Network administration

3. Satellite Teleconferencing, and Web Conferencing (Webinar)

The eLearning staff is responsible for satellite teleconferencing and Web conferencing services at the college. The services are available at the Teleconference Center located in the eLearning Department. The Teleconference Center receives Ku and C-band digital and analog transmissions from all the satellites in North America and is available for use by the community.

4. Location and Hours of Service

The eLearning Department is located in the first floor of the Learning Resource Center (LRC). The eLearning Department Help Desk is available in the office Monday and Tuesday, 8 a.m. – 7 p.m. and Wednesday through Friday, 8 a.m. – 5 p.m. In addition to these office hours, the eLearning Department Help Desk also provides basic services via Email on Saturday and Sunday.

For assistance with any of the resources listed above, call the eLearning Help Desk at ext. 7015 or Email onlinehelp@southflorida.edu.

Contacting the IT Help Desk regarding the resources listed above will only delay service.

Network Systems

The two-way interactive system technical support is provided by the Information Technology Department.

1. Two-Way Interactive System Technical Support

Information Technology staff provides technical support for the two-way interactive system. The Information Technology staff also monitors the system while classes are in session.

2. Hours of Service

See Hours of Service Section 8.2 of this document.

Introduction

Although it may sometimes appear that security was designed to make our lives difficult, it is in all actuality designed to protect us. Security is implemented to protect not only you and your data, but also to protect the information resources and student, employee, and financial data of SFSC.

The chief information officer (CIO) of Information Technology is designated as the IT security administrator for SFSC. What this means is that the CIO is responsible for making sure that our network, servers, and computers are safe from viruses, hackers, and any other risks that may be prevalent in this technological age. If you can identify a security problem, it is your responsibility to notify the security administrator immediately. Do not show or identify the problem to others.

This section is designed to help you understand the intricacies, dangers, and best practices of technology security.

Why is Information Security Awareness Necessary?

The mission of the SFSC's Information Technology Department (IT) is to deliver and maintain an information security program that safeguards information assets against unauthorized use, disclosure, modification, damage, or loss.

This is done by educating the college and non-college people about technology security related issues, assisting in strengthening technical measures to protect campus resources, and developing mechanisms to react to incidents and events that endanger the college's information assets.

With the Internet came the free and unimpeded flow of information and ideas. But, that capability comes with high risk from breaches, hacker attacks, and viruses that can take down the network on which administration, instruction, and communication depend. Our passwords, our Email, business data, student data, our reputation, and everything we do on a computer, are at the mercy of viruses and hackers if they break into our network.

One thing is clear: While the availability of computing resources is critical to the day-to-day operation of the college, network and data security is everyone's responsibility. It would be convenient if the solution was a piece of technology, and it's tempting to rely on the IT staff to ensure cyber security, but the reality is more complex. A successful security strategy involves technology, policy, and people.

How Secure Are You?

If you were going to take down the FBI website, would you do it from your computer using your Internet account? Of course you won't. People who perform computer crime often use innocent victims' computers as go-betweens in their activities. It's like using a stolen car to commit a crime...guess whose license plate gets turned in.

Indiscriminant vandalism of vulnerable computers is common. Automated worms and viruses don't care whose computer they infect. Many times neither do vandals who deface Web pages and access personnel and personal files. They'll take whatever they can get. More and more often, an automated code installs secret back doors allowing other people to control our computers.

Any computer on our college network is an attractive target. Our high speed Internet connection, lack of restrictive communications barriers, and the large number of lightly monitored computers could make our network an attractive storage and dissemination point for pirated software, illegal copies of movies, and various types of inappropriate material.

Physical Security for Technology Resources

Physical security of technology resources is something that can be easily put in place by each and every department and each individual as well. Take the time to be sure physical security is a priority.

You may think that because a computer (or other technology resource) is on your desk, in an office environment, or located in a lab, that it's secure. This is not necessarily correct. Thus, everyone should take precautions to protect against casual theft and unauthorized access. There are a few simple things that can be done to secure such resources:

- Make sure external and internal doors to offices and/or labs are locked at appropriate times -- especially when unattended.
- Follow IT procedures for moving or repairing equipment so it is not taken under false pretenses. Be sure you know who is taking the equipment. See the "Hardware" topic in this document for information on these procedures.
- Either log off or lock the computer if you are going to be away from your area for any length of time: don't give someone the opportunity to misrepresent you on the network by using your ID. Encourage others to do the same.
- Students and/or guests should not be left unsupervised in an area where there are computers.
- When using a laptop computer outside the office, be conscious not to leave it unattended. Confidential information could be stored on the hard drive.

Anti-Virus Software

Every year, people who want to be protected from the latest flu virus get a new flu shot. This is because, every year, new flu viruses appear making the old flu shots ineffective.

Similarly, because new computer viruses are released almost daily, our computers need to get new "shots" almost daily to provide continued protection. This is done by updating our anti-virus software.

However, viruses are getting more sophisticated every day. They can open secret doors allowing strangers into our network. They can send out private information. They can delete files on computers. They get better and better at infecting computers and convincing us to help them do it. They increasingly make a mess of the computers and servers that they infect.

No anti-virus software can protect us from all viruses. Anti-virus software is out of date as soon as a new virus is released. During the hours or days after a new virus is released, all the computers in the world are vulnerable until new anti-virus signatures can be created, distributed, and installed. Thus, even though we're running anti-virus software, it is necessary to use care when opening Email attachments or downloading unknown files.

The anti-virus software that SFSC provides to all of its computers will update itself automatically if the computer is connected to the SFSC network. However, not all computers at SFSC, such as laptops, are always connected to the network and, therefore, must be updated manually and frequently.

Outdated Operating System Software

Have you ever had a computer do something it wasn't supposed to do? Crash or hang up or display something oddly? Ever hear of the term "computer bug"? These are all examples of software defects.

Some software defects can enable thieves, vandals, or automated code to take control of computers. Even brand new computers and software often have defects that are discovered after they were shipped.

Software makers regularly release defect fixes. To protect ourselves, all of the computers connected to the SFSC network are updated automatically. Again, computers that are not always connected to the network, such as laptops, must be updated manually and frequently.

File and Folder Sharing

Current operating systems allow us to share folders on our computers should we wish to do so. Unfortunately, a computer can be unintentionally configured to share files and folders that can give away personal information, passwords, or control of the computer. Make sure you don't give away more than you intend. Here are a few tips.

- Never share an entire hard drive.
- Create specific folders to share rather than sharing existing ones.
- Be careful what you put in shared folders.
- Be careful about letting others store files in your folders without a password. Some folks may put objectionable material there. Also, many viruses can use your folders to spread.
- Never store college documents on systems other than college servers.

Backing Up and Storing Data Files

IT operates a set schedule to backup network servers and the data files contained on them (except the R drive). We maintain several backup copies and store them in a safe place. You will, most likely, have files on your computer's local hard drive. If you do, you have an important responsibility to safeguard it, especially if that data contains sensitive or confidential information. Here are some simple practices to follow to ensure that the data you use on a daily basis is safe.

- Back up your data regularly (at least once a week) to your network drive.
- Know how to restore the backed-up data.
- If you have data on removable media (such as CDs or DVDs), shred CDs and DVDs that may contain outdated sensitive information.
- If you have important and/or sensitive information stored on CD or DVD, lock your backup media in an accessible but secure location such as a filing cabinet (a locked, fire-resistant cabinet if possible). Unless otherwise specified, backups should be accessible to an employee's supervisor, and should be stored in a location that can be available in the event of a disaster.

Welcome to the Internet

We all see reports of theft, vandalism, or fraud on television and in the newspaper.

How often do you think such things would occur if there was little or no risk of getting caught or punished, or if the crime could be performed from halfway around the world using someone else's name - in seconds?

Here are some things to keep in mind about the Internet.

- The Internet is made up of more than 300 million people. There are people out there who will take advantage of you.

- Anyone can put anything they want on a Web page. It doesn't make it true.

- If you put up your own Web page, be careful of the type of personal information you make available to everyone on the Internet.

- When you type passwords or personal information into a website, the information is available to the owner of the website. Only type your SFSC password into official SFSC websites. Doing otherwise gives the owner of the website instant access to all your SFSC accounts.

- If you have access to Web publishing, be careful how you use it. Today's computers make it easy to publish files to the Web with a couple mouse clicks or a simple drag and drop. It is easy to make a mistake. It is very easy to mistakenly publish your "My Documents" folder to the World Wide Web.

Email Usage

Although Email is typically only viewed by you and the recipients of your Email, there should be no expectation that your Email is private. Your Email can be printed, forwarded to other users, etc. by its recipients. Email is to be used in a responsible, efficient, ethical, and legal manner. Your Email should consist of appropriate topics and language that would appear in a formal memorandum or a telephone conversation. As with all other institutional resources, the use of Email must be consistent with the educational mission, goals, and policies of SFSC. See the email section of this document for more information.

Password Protection

Guidelines for Generating a Strong Password:

- Create a password that contains upper and lower case letters. Put the mixed-case within the password; a single change of case at either or both ends may not be sufficient.
- Create a password that mixes letters with digits. Again, place the digits throughout the password, not simply at the beginning and end.
- Create a password that is easy to remember so you don't have to write it down.
- Create a password that you can type quickly, without having to look at the keyboard. This makes it harder for someone to steal your password by watching over your shoulder.
- Choose a line or two from a song, a poem, a literary title, or use an affirmation. Create a password by using the first letter of each word in the title, etc. For example:
  - Title: “I can do anything I set my mind to" becomes **IcDAismMt.**
  - Choose two short words and connect them. For example: "dogboat," "shockvalve," or "candyclown."

Be creative and have fun with it.

WARNING: Do not use these examples!

Guidelines on What to Avoid:

- Avoid using personal information. For example, your name, your user ID, the name of a spouse, child, friend, or pet.
- Avoid using information easily obtained about you, such as license plate numbers, telephone numbers, social security numbers, the brand of your automobile, the name of the street you live on, etc.
- Avoid using a password made of all digits or repeating the same letter to create a password.
- Avoid using a word contained in any dictionary, spelling list, or other word list in any language.
- Avoid using simple transformations of a word such as reversing the spelling, changing upper case to lower case or vice versa, or using all capitalization. To

increase the number of possible password combinations a cracker/hacker would have to guess, be sure to use a password that is at least eight characters long.

Here are some things to remember about passwords:

- **DO NOT** sign on to a computer so that another person may gain access to the network or application systems.
- **DO NOT** write your password on a piece of paper and place it in clear view or under the keyboard or mouse pad. These would be the first places someone would look!
- **DO NOT** disclose your password to any other person.
- **DO NOT** use your SFSC User ID and password on any website other than a SFSC website or page.

Any of the above actions constitutes a security breach and may, if considered serious enough, subject you to disciplinary action.

Why Should I Worry if Someone Has My Password?

Your user ID and password identify you as you to the server. If someone has your password, that person could pretend to be you while doing unauthorized or illegal things online. For example, you may not care if someone reads all of your Email, but you would care if someone were using your account to send Email to organize a crime, send a virus, or send Email with inappropriate material to someone else. You may not care if someone viewed student data, but you would care if someone used your account to change student data or even corrupt student data (your account name would be "attached" to those actions). Also, someone with your password may be able to make your account unusable to you. To protect yourself from unnecessary investigation and frustration, it is a good idea to protect your password.

If there is any indication an account has been accessed illegally or if strange things appear to be happening, **immediately** report it to IT, and **immediately** change your password. Protecting your password is one way you can protect yourself from unauthorized use of your computing accounts and files.

Privacy of Student and Employee Records

In March 2005, a thief stole a laptop computer from a major California university office. That laptop contained personal information of about nearly 100,000 alumni, students, and applicants. The university had to notify almost 100,000 people that social security numbers or other sensitive data had been compromised. You may be thinking about our administrative software system as the sole repository of student and employee information. Not so. Sensitive information may reside on your computer's local hard drive in the form of documents, spreadsheets, and databases. Storing these types of documents in your home or departmental directories on the network instead of your local computer's hard drive may lessen the impact if someone were to abscond with a computer from your office. **DO NOT** store files that may contain sensitive information

on the "Everyone" drive (drive R:) or on any server other than those located at SFSC or under contract with SFSC as these locations are not considered secure.

The college has specific policies and procedures to protect the confidentiality and privacy of student and employee records. South Florida State CollegeProcedure 2152 deals directly with the Family Educational Rights and Privacy Act (FERPA) and Florida Statute1002.22. You are required, as a college representative, to abide by these laws.

Copyright or Copywrong?

Copyright law states that the owner of any tangible creative work has the *sole* right to reproduce, distribute, perform, display, transmit, or transform that work. Therefore, unless you have the permission of the copyright owner or owners, your use or reproduction of the materials constitutes copyright infringement.

Nearly every original, tangible expression is copyrighted immediately upon creation. An author does not have to register the work, announce that the work is copyright protected, or display the copyright symbol to copyright the work. All he or she must do is create an original work in tangible form.

In fact, very little is not copyright protected. Some things that are not included: works that are not in tangible form, titles, names, symbols or designs, ideas, procedures, methods, concepts, and works that are entirely comprised of common property that has no original authorship such as tape measures and rulers, standard calendars, height and weight charts, and so forth. The only other works that are not covered under copyright are works in the public domain.

When in doubt, assume that a work is copyrighted, and you need permission to use it.

The Internet, most software, including freeware, is NOT in the public domain. All software is copyrighted on creation. The only public domain software available is software that the owner has specifically relinquished to the public domain. Other software covered by copyright is:

- commercial software,
- shareware, and
- freeware.

For commercial software and shareware, you may make an archival copy of the software for backup; however, you cannot use the backup unless you need to recover the original. You may not modify or reverse engineer (decompile) the software. You may not develop new software built on these software packages without the permission of the copyright holder.

For freeware, you may make copies for backup and distribution, but not distribute it for profit. You may modify and/or reverse engineer (decompile) the software. You may develop new software built on these software packages provided the new software is also designated as freeware. You cannot modify or further develop freeware and then sell it.

There are specific penalties for violating the copyright law that you and the college could be held accountable for if you were to violate that law. For more information on copyright issues, please refer to the "Software" section in this document.

History: Last Reviewed: October 2011

Adopted: August 2005
Revised: September 2007
Revised: April 2010
Revised: September 2011
Revised: July 2012

Appendix

Acceptable Use of Technology for SFSC Employees

Introduction

SFSC provides computer access and network capabilities through IT. The college relies heavily upon these systems to meet operational, financial, educational, and informational needs. It is essential that these systems and machines be protected from misuse and unauthorized access. It is also essential that SFSC's computers, computer systems, and computer networks, as well as the data they store and process, be operated and maintained in a secure environment and in a responsible manner.

This policy applies to **ALL** SFSC computer systems and refers to **ALL** hardware, data, software, and communications networks associated with these computers. This policy covers all computers ranging from single user personal computers to those connected to the college's network. In addition to this policy, users of these computer systems are subject to applicable state and federal laws.

Computing resources are valuable, and their abuse can have a far reaching negative impact. Computer abuse affects everyone who uses computing facilities. The SFSC community should exercise high moral and ethical behavior in the computing environment.

SFSC's IT staff will not look at private information, unless authorized by an individual to perform work on his or her behalf or under extraordinary circumstances that may require maintaining the functionality of the system. Extraordinary circumstances include, but are not limited to the following: reading the header of an incorrectly addressed Email message to try to send it to the intended recipient, investigations of suspected violations of the college's policies, medical or need-to-know emergencies, financial or legal audits, or when required to comply with law enforcement authorities.

SFSC will only monitor the activities of those that use the campus network or the Internet as it relates to optimizing network performance, unless allegations of improper behavior are brought to our attention by others, or we discover inappropriate activities in the course of investigating problems with network performance. We do routinely monitor traffic levels on the network, to maintain optimal performance, and take note of which individual machines may be generating large volumes of traffic. Routine monitoring is concerned only with load on the network resources and does not seek to eavesdrop on the nature of the information being transmitted.

Policy on the Public Records Law and Email

Florida's Public Records Law

Chapter 119 of the Florida statutes defines public records as:

> "All documents, papers, letters, maps, books, tapes, photographs, films, sound recordings, data processing software or other materials, regardless of physical form or characteristics, or means of transmission, made or received pursuant to law or ordinance or in connection with the transaction of official by any agency."

How the Law Affects College Employees

Email created or received by college employees in connection with official business, which perpetuates, communicates or formalizes knowledge, is subject to the public records law and open for inspection unless specifically exempted by the legislature.

If your Email falls within the definition of a public record, you may not delete it except as provided by the State General Records Schedule for Community Colleges (Schedule GS5). Furthermore, unless your Email is specifically exempt as described by the public records statute, you must produce that Email to any person upon request.

Retention Periods for Public Records

Retention periods for public records, including Email can be found in the State General Records Schedule for Community Colleges (Schedule GS5). Retention for most Email records falls within the following two categories:

1. **Retain Until Administrative Purpose is Served:**
   - Routine announcements and information including notices of seminars and workshops, queries regarding processes or ideas, and general information regarding programs;
   - Reference files that are general-information files used in daily functions of the administrative area; and
   - Meeting notices, minutes, statistical records, reading files, and recipient's inter-departmental memoranda.

Retention schedules are based on a record's informational content, not its format. Email that falls into the category of "retain until administrative purpose is served" may be deleted on a daily basis. Email that has a longer retention period – such as correspondence or sender's memoranda – must be kept through the three-year retention period.

2. **Retain for Three Fiscal Years:**
   - General correspondence, sender's inter-departmental memoranda, and most fiscal and budget records.

It is the user's responsibility to know which category Email falls. When in doubt whether to delete or archive your Email messages, contact your department chair or administrator.

South Florida State College
Technology Usage Guidelines and Support Manual
Acceptable use Policy

Guidelines

It is a general policy that technology resources are to be used in a responsible, efficient, ethical, and legal manner in accordance with the mission of SFSC.

Failure to adhere to the policy and guidelines may result in suspension or revocation of the offender's privilege of access to technology resources.

Access to technology resources is coordinated through a complex association of local hardware and software as well as external government agencies and regional and state networks. In addition, the smooth operation of the network relies upon the proper conduct of the end users who must adhere to strict guidelines.

1. Acceptable Use – The use of your account must be in support of education and research that is consistent with the educational goals and policies of SFSC. Use of other networks or computer resources must comply with the rules appropriate for that network. Transmission of any material in violation of any U.S. or state regulation is prohibited. This includes but is not limited to: violating the conditions of the Educational Code dealing with the student's rights to privacy, copyrighted material, threatening or obscene material, or material protected by trade secret. Use for product advertisement, political lobbying, personal or private business, commercial or for-profit purposes are also prohibited.

2. Privileges – The use of technology resources and the Internet at SFSC is not a right but a privilege and inappropriate use will result in a cancellation of that privilege. Each individual who receives an account will receive information pertaining to the proper use of the network. SFSC administrators will decide what inappropriate use is and their decision is final. An account may be closed by the administration at any time deemed necessary or recommendation of the faculty or staff.

3. Email "Netiquette" – You are expected to abide by the generally accepted rules of network etiquette. These include (but are not limited to):
    a. Be polite. Do not use vulgar or abusive language.
    b. Exercise caution revealing personal information over the Internet. Email is not guaranteed to be private.

4. Warranties – Since Internet connectivity is provided by a third party, SFSC cannot control certain service interruptions. Use of any information obtained through this Internet connection is at your own risk. SFSC specifically denies any responsibility for the accuracy or quality of information obtained through its services.

5. Authorization and Security – Security on any computer system is a high priority. If you can identify a security problem, you must notify the security administrator immediately. Do not show or identify the problem to others. Do not allow your

account to be used by another individual. Do not use another individual's account. Attempts to log on as another user may result in cancellation of your privileges. Any user identified as a security risk or having a history of problems with other computer systems may be denied access. All individuals should not reveal their private address or phone number or those of others over the Internet. Each user (student, faculty, staff, or authorized others):

a. must have a valid, authorized account in areas required and computer resources which are specifically authorized;
b. may only use his/her account in accordance with its authorized purpose;
c. may not allow other persons to use his/her account unless authorized by the system administrator for a specific purpose;
d. is responsible for safeguarding his/her own computer accounts; and
e. should change passwords often to ensure privacy and security.

6. Vandalism – Vandalism will result in cancellation of your privileges. Vandalism is defined as malicious attempt to disrupt network services, harm or destroy data of another user, or disrupt Internet services. This includes (but is not limited to):
    a. the creation of, or the uploading of, computer viruses on the network or Internet;
    b. the installation of software products that monitor network activity;
    c. the installation of software products that monitor and/or record computer activity;
    d. violation of copyright or patent laws concerning computer software, documentation, or other tangible assets.

7. Exceptions of Terms and Conditions – All terms and conditions are stated in this document are applicable to all users of the network. These terms and conditions reflect an agreement of the parties and shall be governed and interpreted in accordance with the laws of the state of Florida and United States of America.

The above Acceptable Use Policy and Guidelines have been established by SFSC. If any user violates any of these provisions, his or her access to the network may be terminated and all future access could possibly be denied.

Acceptable Use of Cloud Computing at SFSC

The *Acceptable Use of Cloud Computing* section of this policy provides guidance to members of the SFSC community who wish to use applications and services available on the Web, including social networking applications and content hosting. These tools, which often reside on complex, dynamic networks, are collectively referred to as "cloud computing."

Internet Applications at SFSC

Internet application and service providers may require users to consent to their Terms of Service, frequently via a "click-through" agreement, which is a legal contract. Faculty, staff, and students are not authorized to enter into legal contracts on behalf of SFSC and may not consent to click-through agreements for the purposes of college business. If individuals approve these agreements, they would be personally responsible in any legal actions related to the services.

College information **must not be stored, shared, or otherwise processed** by a cloud computing service unless the service enters into a legally binding agreement with SFSC (e.g., D2L – Panther Den) which is considered a private cloud computing service that requires the provider to protect and manage the data according to standards and procedures acceptable to the college.

SFSC provides a variety of applications and services that support instructional, administrative and academic research activities by faculty, staff and students while meeting the college's guidelines. SFSC may have agreements with specific vendors or offer college-hosted solutions that meet your needs. Check with IT for a list of existing campus agreements and services.

Challenges with Cloud Computing

Applications and services that are not purchased or licensed by SFSC – including those freely available on the Internet, such as popular social media sites – may not meet college standards for user privacy, security, intellectual property protection, and records retention.

Potential problems with non-SFSC approved applications include:

Intellectual Property and Copyright

Terms of Service from many providers include provisions about who owns intellectual property rights when content is created or uploaded to the application or service that may confuse intellectual property ownership claims.

Note, also, that cloud computing providers may reserve the right to change their Terms of Service at will.

Privacy and Data Security

Security of data uploaded to Internet services is rarely guaranteed. "Free" services frequently depend on data aggregation and data mining about users to attract advertising revenue. The privacy and/or security of that data is then potentially at risk. State and federal law mandate protection of sensitive information such as student data, social security numbers and credit card information.

The college has specific policies and procedures to protect the confidentiality and privacy of student and employee records. SFSC Procedure 2152 deals directly with maintaining the integrity and security of electronic student records including the Family Educational Rights and Privacy Act (FERPA) and Florida Statute 1006.52. You are required, as a college representative, to abide by these laws.

Data Availability, Accessibility and Records Retention

All SFSC business and educational records are subject to public records law, regardless of where they are stored. However, many providers assume no responsibility for archiving content or ensuring availability, which places the burden on the user to ensure availability.

Additionally, SFSC is committed to ensuring that information, including any materials provided through Internet applications and services, meet reasonable standards of accessibility for all.

SFSC also requires that instructional and administrative records be retained according to the retention periods for public records, as published in the State General Records Schedule for Community Colleges (Schedule GS5).

Best Practices for Using Cloud Computing

Sensible practices apply when using any Internet application.

Intellectual Property and Copyright

- Remember that many SFSC images and symbols are owned by the college and not freely available for reproduction. Contact Community Relations and Marketing for more information.

- Remember that students, except in a limited number of circumstances, own their work.

- Ensure that students understand appropriate use of copyrighted materials, particularly when content is publicly available.

Privacy and Data Security

- Never divulge information that the college has classified as "restricted" on the Internet. Examples include social security numbers, credit card information, and driver's license numbers. Do not place college data on a **public** cloud computing site.

- Comply with FERPA requirements to protect student privacy. Do not place grades or evaluative comments on Internet sites other than Panther Den (D2L). Contact the Office of the Registrar for assistance interpreting FERPA

- Never use personally identifying information without explicit permission, unless the college has classified the information to be "public," for example, in the college directory ("People Directory").

Data Availability and Records Retention

- Do not place college data on a **public** cloud computing site.
- Ensure that all data – whether instructional, administrative, or academic research – are retained according to the records retention schedule.
- Ensure that applications or services are accessible to all.
- Back up materials regularly to ensure that records are available when needed, as many providers assume no responsibility for data-recovery of content.

Tips for Faculty

- Communicate the issues, conditions, and risks associated with any tool you choose at the beginning of the academic term, preferably in the syllabus. This allows students who object to withdraw from the course or to request alternate assignments or other solutions. However, be sensitive to the fact that withdrawal may not be possible if the course is required, the course is offered in a sequence, the course is not offered regularly, or the course is only offered by one instructor.
- Restrict online access to student content as much as possible within the context of your instructional goals. In general, coursework conducted online should always be restricted to members of the course.
- Always require students to use aliases when creating accounts, particularly if access to student work is public. Also, prohibit use of the SFSC Internet name and password as an alias.
- Never include personally identifying information about yourself or your students in content or in profile information online.
- Remember that faculty, students and staff may not speak for the college.
- Manage your social media presence strategically and review it regularly.

Copyright and Licensing Agreements

Most software has a copyright notice and a license agreement. SFSC must comply with both of these. Since there can be several penalties for breaking copyright procedures or license agreements, read and understand them for each piece of software you use.

You should also read and understand the following information that applies to copyrights and the penalties for violating laws regarding them:

> "Software is automatically protected by federal copyright law from the moment of its creation. The rights granted to the owner of a copyright are clearly stated in the Copyright Act, Title 17 of the US Code. The Act gives the owner of the copyright "the exclusive rights" to "reproduce the copyrighted work" and "to distribute copies…of the copyrighted work" (Section 106). It also states that "anyone who violates any of the exclusive rights of the copyright owner…is an infringer of the copyright" (Section 501), and sets forth several penalties for such conduct.
>
> Those who purchase a license for a copy of software do not have the right to make additional copies without the permission of the copyright owner, except (i) copy the software onto a single computer and (ii) make "another copy for archival purposes only," which are specifically provided in the Copyright Act (Section 117). The license accompanying the product may allow additional copies to be made; be sure to review the license carefully.
>
> Software creates unique problems for copyright owners because it is so easy to duplicate, and the copy is usually as good as the original. This fact, however, does not make it legal to violate the rights of the copyright owner. Although software is a new form of intellectual property, its protection is grounded in the long-established copyright rules that govern other more familiar media, such as records, books, and files.
>
> The unauthorized duplication of software constitutes copyright infringement regardless of whether it is done for sale, for free distribution, or for the copier's own use. Moreover, copies are liable for the resulting copyright infringement whether or not they knew their conduct violated federal law. Penalties include liability for damages suffered by the statutory damages of up to $100,000 for each work infringed.
>
> The unauthorized duplication of software is also a federal crime if done "willfully and for purposes of commercial advantage or private financial gain (Title 18 Section 2319(b)." Criminal penalties include fines of as much as $250,000 and jail terms of up to five years.

Technology and Innovation Assessment Process

General Purpose Statement

The purpose is to explain the process for identification, evaluation, and assessment of technology and innovation to determine viability for integration into South Florida State College's (SFSC) learning environment and existing technology infrastructure.

Glossary of terms

Compatibility – capability of two or more items or components of equipment or material to exist or function in the same system or environment without interference.

Security – measures and controls that ensure confidentiality, integrity, and availability of information technology assets. This includes hardware, software, firmware, and information being processed, stored, and communicated.

Support – includes installation, maintenance, and upkeep of technology by the Information Technology (IT) department.

Technology – all components of informational technology used in the delivery of educational or administrative materials which includes, but is not limited to, software, hardware, and Internet applications or activities.

Hardware – includes, but is not limited to, all types of computers, monitors, media equipment, printers, copiers, telecommunications equipment, as well as smaller peripheral equipment such as keyboard, mouse, label maker, mobile devices, etc.

Innovation – use of Internet applications and activities in the delivery of educational or administrative materials which includes, but is not limited to, cloud computing, social networking, and other Web 2.0 resources.

Web 2.0 - new generation of Web services and applications with an increasing emphasis on human collaboration. Most commonly associated with web applications that facilitate interactive information sharing, interoperability, user-centered design, and collaboration on the World Wide Web.

Communication Flow for Technology/Innovation based Assessment Requests

All standard hardware and software purchases must be approved by IT before purchase as identified in SFSC Procedure 4040.
Faculty developing online courses must follow the process identified in the SFSC eLearning Handbook.

South Florida State College
Technology Usage Guidelines and Support Manual
Technology and Innovation Assessment Process

The communication process for any individual or department considering technology/innovation not currently provided ***and/or supported*** by the college is as follows:

1. Consult with department head/dean.
2. Complete Request for Software and Hardware Assessment (RSHA) form. Web 2.0 resources assessment requests may require additional clarification.
3. Submit RSHA to the chief information officer (CIO) for review.
4. If the request requires further review, the CIO will forward the RSHA to the Technology Committee. If no further review is required, then step 6.
5. The Technology Committee will evaluate the request to ensure the technology innovation assists in accomplishment of the college's strategic goals. If approved, then step 6.
6. IT will analyze the best way to proceed technologically and communicate with other departments for additional input as needed.
7. IT staff will advise the requestor approximately how much funding is needed.
8. The requesting department will complete the requisition/purchasing process, if applicable, as identified in SFSC Procedure 4040.
9. IT and/or e-Learning will continue with project if funded.

The requesting department should not order or imply that SFSC will purchase or consider utilization of any technology until IT is involved with the discussions. IT must ensure the new technology is compatible with our existing environment, can be supported by IT, and is secure.

South Florida State College

Request for Software or Hardware Assessment

Standard software and hardware purchases should follow the procedure identified in the SFSC Technology Support Manual and SFSC procedure 4040.

This form is to be used by any individual or department considering technology/innovation not currently provided ***and/or supported*** by the College. Please follow Steps 1-3 of the **Technology and Innovation Assessment Process** document.

Part I – To be completed by all requestors
Requestor
Name: _____

Email: _____

Department: _____

Software (includes free software, Internet applications, and Web 2.0 resources)
Complete all applicable information.

Name: _____

Briefly describe the software's purpose/functionality. _____

_____

List the SFSC-owned software packages which have a similar purpose or functionality. Identify the essential differences which require this package to be purchased.

_____

_____

_____

_____

List other individuals/departments currently using existing software (if not site licensed, e.g., Office, Adobe)

_____

_____

Hardware

Description:_____

New (additional)_____ Replacement _____

Justification for Request:

This request benefits the following: (may select more than one)

Individual_____ Department_____Various Departments_____

Describe _____

This request benefits students:

Directly_____Indirectly_____
(Complete Part III if this benefits students directly.)

Have funds been budgeted for this purchase? Yes ___ No___ (if no complete Part II)

Part II – Cost and Funding – To be completed if purchase has not been budgeted

Cost (To be completed by requestor and department/program chair/director/dean)

Estimated Cost of Requested Item(s) include maintenance/renewal fees if applicable:

Price listed by vendor, website, IT quote, etc. _____

Funding Source _____ Fiscal year _____

Budget Manager for funding source _____

Part III – To be completed for software used in courses

Benefit

For each course which will use this software, complete the following:

Describe how the software supports the course's learning outcomes

_____

Number of students per annual _____

List your department/division faculty who would be/are interested in using this software or need to know when it is upgraded.

_____

Part IV – To be completed by all requestors

Which South Florida State College's Strategic Imperative Goal(s) would the approval of this request fulfill? _____

_____

The requesting department should not order or imply that SFSC will purchase or consider utilization of any technology until IT is involved with the discussions. IT must ensure the new technology is compatible with our existing environment, can be supported by IT, and is secure.

Signatures

Requestor _____ Date: _____

Department/Program Chair _____ Date: _____

Dean/Director _____ Date: _____

Forward this request to the Chief Information Officer for review and consideration. You will be notified when review of your request is completed.

For IT office Use Only

Review Date _____

Approved _____

Referred to Technology Committee _____

Requires Additional Clarification _____

Not Approved _____

Table of Contents

I. Introduction

II. Instructional Use of Social Media – Preparation

III. Instructional Use of Social Media – Special Concerns

IV. Representing SFSC Officially on Social Media Sites

V. Best Practices

VI. Moderating Comments on Social Media Sites

VII. Resources

VIII. References

South Florida State College
Technology Usage Guidelines and Support Manual
Social Media Guidelines

I. Introduction

As social media evolve, South Florida State College(SFSC) employees and students are engaging in new methods of communication, internally and externally. With new opportunities for communication and collaboration come further responsibilities.

SFSC has crafted guidelines to clarify how to enhance and protect personal and professional reputations as well as the college's image when participating in social media.

Social media are Web-based tools, also known as cloud computing, that can provide immediate publication of content to the Web and enable interaction between the person posting the message and her/his audience. Examples are blogs (Blogger, WordPress), micro-blogs (Twitter), social networking sites (LinkedIn, Facebook, MySpace, Google+), wikis (Wikipedia), photo sharing sites (Flickr, Picasa), and video sharing sites (YouTube).

These guidelines are for SFSC faculty, staff, and administrators; students acting as official SFSC representatives; and contractors creating or contributing both on and off www.southflorida.edu.

When using social media in professional and institutional roles, employees and students should follow the same behavioral standards as they would in everyday life offline. The same laws, professional expectations, and guidelines for interacting with students, parents, alumni, donors, media, and other college constituents apply to social media as they do in everyday life. Employees and students are liable for anything they post to social media sites.

This set of guidelines is a living document and will be periodically updated to reflect current trends, norms, and best practices in the use of social media.

II. Instructional Use of Social Media – Preparation

A. Although various social media can be used to foster a sense of community and motivate students, it is preferred that instruction take place in Panther Den (D2L), the classroom, or using other media provided and supported by SFSC. These locations provide security within the college environment.

B. When a social media application offers the option, instructors should use a private page, e.g., Facebook group, which can only be joined by invitation. Such measures protect students from some online risks.

C. Some social media may stipulate that content posted on their sites becomes their property; therefore, users should think carefully about giving up intellectual property rights--a user's posted content could potentially show up on the Internet. Instructors should discuss this concern with students.

D. Instructors should provide students with

1. Written instructions, or a link to instructions within the application, regarding how they can safeguard privacy and report abusive content.
2. A disclaimer noting that any product advertised on the site is not endorsed by the college or instructor.
3. A disclaimer noting that opinions expressed do not reflect opinions or policies of the college.
4. A reminder that social media sites' policies on privacy and other issues change often and that students should check sites regularly for updates.
5. A statement that postings may be removed by the page owner at any time (when the tool allows this action).
6. A statement that the page administrator may block user posts (when the tool allows this action).
7. A statement that all content must comply with the college's Technology Usage Guidelines.

The following is a sample paragraph for course handouts that addresses items above. Instructors must advise students of these issues, but the wording is optional.

> I invite you to join the class (Facebook/Twitter/etc.) site. Participation is voluntary, and the purpose is to form a community of learners and to provide extra resources and information that enrich the class experience. Please be sure to view this site, _____, which explains the current privacy settings and policies associated with (Facebook/Twitter/etc.). These policies may change frequently and without notice. Be sure to check this page regularly.
>
> Please note that any harassing posts and any posts violating SFSC's Technology Usage Guidelines will be removed, and those users may be blocked. Comments posted on this site do not reflect SFSC's views. Products advertised are not endorsed by the college.

The suggested syllabus statement regarding social networking:

> This class uses social media to build community and enrich students' overall experience. Participation in this site is optional and not a required element of the class. All essential course information will be presented in [the classroom or in Panther Den (D2L)]. The instructor takes careful precautions to safeguard students on the Internet; however, as with many Internet interactions, risks still exist. By choosing to participate on the class' social media site, you accept responsibility for the information you post and assume the risks associated with the use of social media.

E. Effective use of social media requires that the instructor check the site *daily* and update it at least *weekly*. Untended sites will be abandoned by users.

F. Instructors who set up instructional pages using social media accept complete responsibility for maintenance of these sites.

G. Students should be instructed about the special requirements of the populations with which they are working, e.g., the Health Insurance Portability and Accountability Act (HIPAA) for nursing students and the Family Educational Rights and Privacy Act (FERPA) for teacher education students.

H. All students should be instructed on social media etiquette and about information regarding their classmates that they should not disclose (see III.B.).

III. Instructional Use of Social Media - Special Concerns

A. When using social media sites in discharging college duties, instructors should ensure that the online presence reflects the professional standards of SFSC; complies with applicable federal and state regulations regarding student privacy; and adheres to college policies and procedures. These include but are not limited to FERPA, HIPAA, SFSC Technology Usage Guidelines, copyright, proper use of college symbols/logos, etc. Instructors should contact the SFSC Community Relations and Marketing Department to ensure that the college brand is consistent.

B. The following information about students should ***never*** be communicated via a social media site:

Grades or test scores
GPA
Academic standing
Attendance habits
Time/day/location/course names of student's current classes
Social security number
Student ID number
Email address
Birth date
Telephone number
PIN number
Disability status
Marital status
Disciplinary actions
Financial aid status
Financial obligations owed

C. Student participation in course social media sites must be voluntary and may not be a course requirement. Instructors should not disseminate essential class information *solely* through a social media tool, any more than they would share such information with only one or two students during office hours. The social media site should enrich the class, not substitute for it or for other college communication methods, including Email.

D. In the case of Facebook, instructors may not employ their own *personal* social media pages for instructional use. They must develop and maintain a separate instructional page, such as a group page. Instructors may not link to their personal social media pages from their instructional social media page or a college website, (i.e., may not "solicit" friends/fans for a personal page from a college website or social media site used for a college class).

E. Be aware of the impact of intellectual property rights and copyrights on information being posted. Always ensure that proper permissions have been obtained for any course or research material being posted to websites. Where images and videos are posted, it may be necessary to obtain permission from individuals identifiable in the image or video.

IV. Representing SFSC Officially on Social Media Sites

If you post on behalf of an official college unit, you are required to adhere to all guidelines and best practices presented in this document. If you are using social media for instructional use, see the sections above, "Instructional Use of Social Media."

A. If you are representing SFSC when posting on a social media site, clearly identify your affiliation with the college.

B. SFSC organizational units that are creating social media sites should consider their messages, audiences, and goals, as well as a strategy for keeping information on social media sites up-to-date. Communicate college-related content only.

C. Whenever possible, link back to the SFSC website. Posts should be brief, redirecting a visitor to content that resides within the SFSC Web environment. When linking to a news article about SFSC, use a news release that resides on the SFSC website instead of to a publication or other media outlet, if possible. SFSC maintains archived stories on its website.

D. Posts on social media sites should protect the college's institutional image by remaining professional in tone and in good taste. No individual SFSC organizational unit should construe its social media site as representing the college as a whole. Consider this when naming pages or accounts, selecting a profile picture or icon, and selecting content to post – all of these should clearly reflect the particular department or unit rather than to the institution as a whole.

E. If you create promotional (non-instructional) multimedia to post, have it reviewed by the Community Relations and Marketing Department. Videos and other online multimedia follow the same guidelines for approval as other communication products via this department. The intention is not to stifle creativity, but rather to ensure that content represents the college accurately and in accordance with institutional branding.

F. College employees who serve as advisors to SFSC student clubs and organizations are expected to follow these guidelines and discuss them with members of the group they counsel.

G. Do not post confidential or proprietary information about SFSC, its students, employees, former employees, or alumni. Employees must follow federal requirements such as FERPA and HIPAA and adhere to all SFSC privacy and

confidentiality policies (see Resources section). Employees who share confidential information risk disciplinary action or termination.

H. When posting, understand and abide by the copyright and intellectual property rights of others and of SFSC. (See Resources section.)

I. Do not use SFSC logos or any other college images or iconography on personal social media sites or sites that have not been given formal permission to represent SFSC through social media. Do not use SFSC's name to promote a product, cause, or political party or candidate.

J. In accordance with college policy, SFSC's computers are reserved for college-related business and carrying out the institution's mission, goals, and objectives.

K. Departments or college units that have a social media page or would like to start one should complete the Social Media Account Request form and submit it to the Community Relations and Marketing Department. Community Relations staff will ensure that all institutional social media sites coordinate with other SFSC sites and their content. All institutional pages must have an appointed employee who will be responsible for content. Ideally, this should be the head of the college unit. Designate at least one other full-time employee who will responsible for posting messages.

V. Best Practices in Social Media Use

This section applies to those posting on behalf of an official SFSC organizational unit, though the guidelines may be helpful for anyone posting on social media in any capacity.

A. Please review the Acceptable Use of Technology for SFSC Employees, which presents a section on cloud computing best practices (http://www.southflorida.edu/_documents/IT_AcceptableUseTechnology.pdf).

B. The world of social media provides no privacy. Consider what could happen if a post becomes widely known and how that may reflect on the person posting the message and SFSC. Search engines can turn up posts years after they are created, and comments can be forwarded or copied. If you wouldn't make a comment at a conference or to the media, or you wouldn't want your family or a prospective employer to see it, consider whether you should post it online. If you are unsure about posting something or responding to a comment, ask your supervisor for input or contact the director, Community Relations and Marketing Department, at ext. 7251.

C. Strive for accuracy, especially when posting on behalf of SFSC. Get the facts straight before posting them on social media. Review content for grammatical and spelling errors.

D. Understand that content contributed to a social media site could encourage comments or

discussion of opposing ideas. Responses should be considered carefully in light of how they would reflect on the person posting and/or the college.

E. Be aware that a presence in the social media world easily can be made available to the public at large. This includes prospective students, current students, current employers and colleagues, and peers. Consider this before publishing to ensure the post will not alienate, harm, or provoke any of these groups.

F. Pay careful attention to the terms of service (TOS) and privacy policy of any social media you consider using. Facebook TOS can be found at http://www.facebook.com/terms.php and its privacy policy is at http://www.facebook.com/policy.php. Twitter TOS can be found at https://twitter.com/tos and its privacy policy is at http://twitter.com/privacy.

G. On personal sites, identify your views as your own. If you identify yourself as an SFSC faculty or staff member online, be clear that the views expressed are not necessarily those of the institution. Personal sites should never be used for instructional purposes.

H. Protect your intellectual property. Visitors can easily pluck photographs/images from social media sites and use them for their own purposes. Consider adding a watermark and/or posting images at 72 dpi and approximately 800x600. Images at that size are sufficient for viewing on the Web, but not suitable for printing.

I. Exercise caution to avoid “phishing” attempts, which aim to gain control of a personal or institutional social media site by deceiving a user into revealing the account’s user name and password. Monitor your social media site to ensure you notice quickly if an unauthorized person gains access.

VI. Moderating Comments on Social Media Sites

SFSC encourages its various audiences to share their thoughts with one another by commenting on a story, feature, tweet, or post. Feel free to use the following guidelines when moderating comments on your site.

A. Comments must be constructive, relevant to the topic discussed, and to the point.

B. Posts that are off-topic, are abusive, are threatening in tone, or contain profanity will be deleted.

C. Excessively long comments may be edited for length, clarity, and space limitations.

D. Anonymous comments will not be published.

E. Posted links must include your name and explain where your link goes, especially if you are directing viewers to a for-profit organization. This is to distinguish spam from legitimate opportunities for the SFSC community.

F. SFSC reserves the right to review all comments and remove comments that violate any of the conditions noted above.

VII. Resources

SFSC Policies, Procedures, and Guidelines

Acceptable Use of Technology for SFSC Employees – http://www.southflorida.edu/_documents/IT_AcceptableUseTechnology.pdf

Technology Usage Guidelines - http://www.southflorida.edu/_documents/Technology-Usage-Guidelines.pdf

Technology Support Manual - http://www.southflorida.edu/_documents/Technology-Support-Manual.pdf

Copyright Laws and Penalties - http://www.southflorida.edu/policy/copyright.aspx

SFSC Policies – http://www.southflorida.edu/_documents/polall.pdf

Policy 1.14	Copyright
Policy 1.16	Intellectual Property
Policy 3.01	Academic Freedom and Freedom of Expression
Policy 2.09	Course Policy Statement
Policy 5.21	Responsibility of Faculty, Professional, Career, and Administrative Staff
Policy 6.01	Electronics Access Use

SFSC Procedures - http://www.southflorida.edu/_documents/proall.pdf

Procedure 1140	Copyright Compliance
Procedure 2090	Development of All Non-Classroom College Publications
Procedure 2100	Release of Information to the Public
Procedure 2158	Information Security
Procedure 3010	Freedom of Expression and Freedom of Express Guidelines
Procedure 6011	Student Access to Technology Resources

State and Federal Law

Family Educational Rights and Privacy Act (FERPA) - http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html
Health Insurance Portability and Accountability Act (HIPAA) – http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html
Sunshine Law - http://www.myflsunshine.com/sun.nsf/sunmanual
U.S. Patriot Act - http://www.justice.gov/archive/ll/highlights.htm

VIII. References

SFSC respectfully acknowledges using portions of the following institutions' documents in the development of the SFSC Social Media Guidelines.

Northwest Florida State College
Ball State University
Pacific University Oregon
Seattle University
Seminole State College