

## *Acceptable Use of Technology for SFCC Employees*

### **Introduction**

SFCC 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 SFCC'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** SFCC 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 SFCC community should exercise high moral and ethical behavior in the computing environment.

SFCC'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 e-mail 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.

SFCC 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 E-mail**

#### *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**

E-mail 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 e-mail 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 e-mail is specifically exempt as described by the public records statute, you must produce that e-mail to any person upon request.

### ***Retention Periods for Public Records***

Retention periods for public records, including e-mail can be found in the [State General Records Schedule for Community Colleges \(Schedule GS5\)](#). Retention for most e-mail 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. E-mail that falls into the category of “retain until administrative purpose is served” may be deleted on a daily basis. E-mail 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 e-mail falls. When in doubt whether to delete or archive your e-mail messages, contact your department chair or administrator.

## **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 SFCC.

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 SFCC. 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 SFCC 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. SFCC 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. **E-mail "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. E-mail is not guaranteed to be private.
4. **Warranties** – Since Internet connectivity is provided by a third party, SFCC cannot control certain service interruptions. Use of any information obtained through this Internet connection is at your own risk. SFCC 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 SFCC. 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 SFCC*

The *Acceptable Use of Cloud Computing* section of this policy provides guidance to members of the SFCC 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 SFCC*

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 SFCC 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 SFCC (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.

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

SFCC 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 SFCC 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 SFCC 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.