ADMINISTRATIVE REGULATIONS
TABLE OF CONTENTS

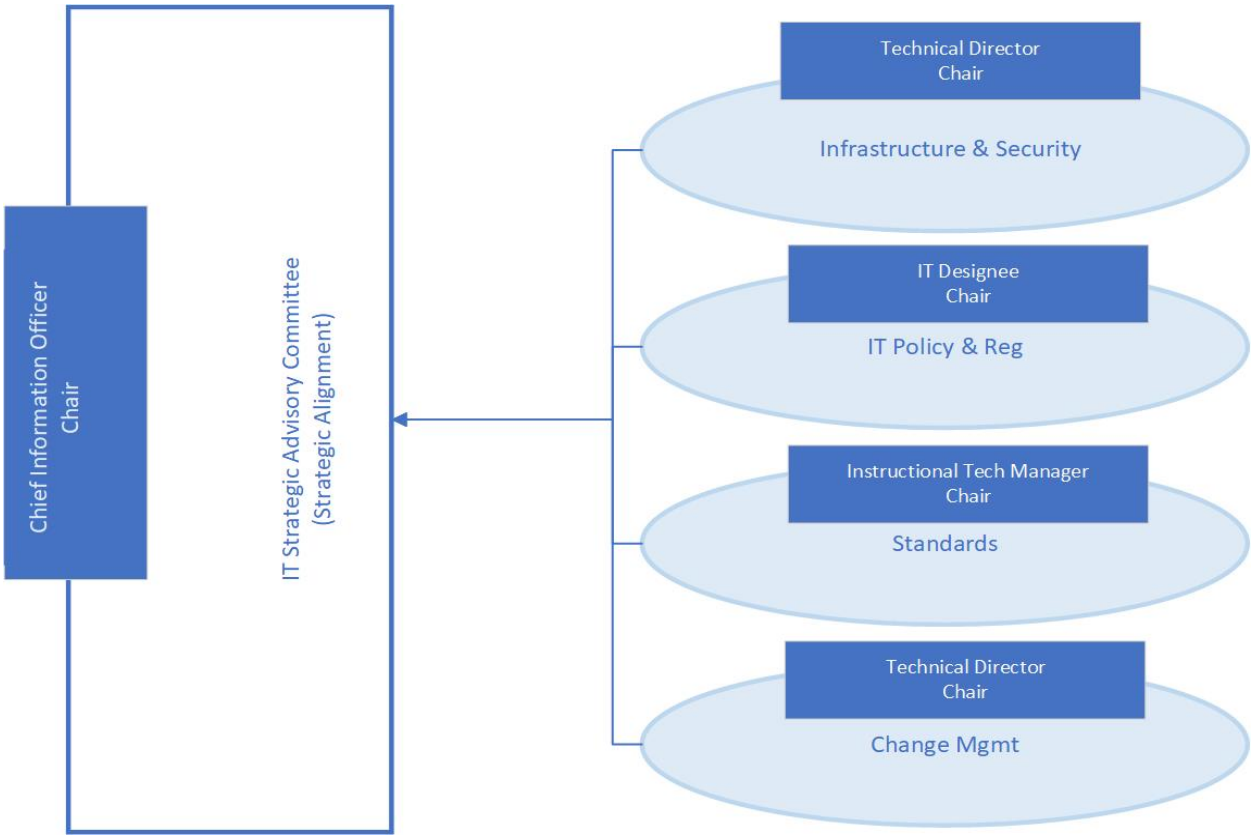
INFORMATION TECHNOLOGY **Regulation 8100**

Introduction and Governance

The Board of Trustees authorizes the use of information technology to support an effective and efficient environment for high-quality instruction and information and to Enhance communication, access, and the College's ability to meet the needs of students and other stakeholders.

The Information Technology Strategic Advisory Committee (ITSAC) provides institutional strategic alignment by establishing priorities and recommend policies and regulations, and is accountable and transparent to the college community. The ITSAC, including subcommittees, advises the Chief Information Officer. The Chief Information Officer submits recommendations to the President, the Executive Leadership Team, or College Council as appropriate.

IT Governance is comprised of the main governing body (ITSAC) and subcommittees. The actions of the subcommittees are recommendations to the ITSAC. This committee shall meet monthly to review all recommendations of the subcommittees. The structure is as follows:



1. Information Technology Strategic Advisory Committee
2. Infrastructure and Security
3. IT Policy and Regulations
4. Standards
5. Change Management

Additional adhoc task forces may be formed for special purposes.

The IT governance structure and responsibility:

1. Information Technology Strategic Advisory Committee (ITSAC)
    a. Meeting frequency: monthly.
    b. Chairperson: Chief Information Officer
    c. Agenda: Developed by chairperson, distributed two days prior to scheduled meeting.
    d. Document and review IT Service Catalog.
    e. Overseeing the development and prioritization of a two-year technical roadmap.
    f. Routinely measuring and monitoring the Return on Investment (ROI) of new and ongoing technology service or solution initiatives.
    g. Review and approval of recommendations of subcommittees for alignment with IT tactical and strategic plans, as well as institutional strategic plan and initiatives.
    h. Document and submit committee recommendations to the president, Executive Leadership Team (ELT), or College Council as appropriate.
2. Infrastructure and Security (ITSAC-I)
    a. Meeting frequency: monthly or as needed.
    b. Chairperson: IT Technical Director
    c. Agenda: Developed by chairperson, distributed two days prior to scheduled meeting.
    d. Develops, recommends and evaluates technologies for the development, support, management, and maintenance of the college IT infrastructure.
    e. Creates task forces to investigate and to develop recommendations for college-wide IT infrastructure initiatives, when appropriate or necessary.
    f. Identifies and assesses college cyber security, privacy and compliance needs and assist with their development and implementation.
3. IT Policy and Regulations (ITSAC-P)
    a. Meeting frequency: quarterly, or as needed.
    b. Chairperson: IT Designee
    c. Agenda: Developed by chairperson, distributed two days prior to scheduled meeting.
    d. Evaluates, authors, reviews, and recommends to ITSAC information security regulations that address risk and align with applicable federal and state regulations, as well as college policy, insurance and compliance requirements.

   e. Evaluates, authors, reviews, and recommends to ITSAC technology use regulations that address risk and align with applicable federal and state regulations, as well as college policy, insurance and compliance requirements.
   f. Evaluates, authors, reviews, and recommends to ITSAC enterprise applications use regulations that address risk and align with applicable federal and state regulations, as well as college policy, insurance and compliance requirements.
   g. Evaluates, authors, reviews, and recommends to ITSAC instructional and academic technology regulations that address risk and align with applicable federal and state regulations, as well as college policy, insurance and compliance requirements.
   h. Create task forces to investigate and develop recommendations for policy and regulation on new or emerging technologies, when appropriate or necessary.
4. Standards (ITSAC-S)
   a. Meeting frequency: quarterly, or as needed.
   b. Chairperson: Instructional Technology Manager
   c. Agenda: Developed by chairperson, distributed two days prior to scheduled meeting.
   d. Supports the development and maintenance of standards that enable a college-wide technology deployment that can be efficiently and strategically managed.
   e. Establishes standards that formally guide the acquisition, maintenance and operations of information technology systems and infrastructure to make sure they are available, secure, cost effective and interoperable (as appropriate to business and academic requirements).
   f. Create task forces to investigate and develop recommendations for college-wide IT hardware, software, and infrastructure initiatives, when appropriate or necessary.
5. Change Management (ITSAC-C)
   a. Meeting frequency: Monthly, or as needed.
   b. Chairperson: IT Technical Director
   c. Agenda: Developed by chairperson, distributed two days prior to scheduled meeting.
   d. Ensures that standardized methods and procedures are used for technical changes.
   e. Minimizes the impact of change-related incidents upon service quality, and consequently improves the day-to-day operations of the organization.
   f.

IT Governance Values

The IT governance committees will use the RACI responsibility model.

- R – Responsible: Governance structure must focus on decision-making and results more so than implementation and project management.
- A – Accountable: Committees and task forces must be held accountable for delivering on their responsibilities. Clear escalation paths for issue resolution must be defined and outlined in charter documentation.

- C – Consulted: Governance committees work with and in all areas of the college with the purpose of understanding expectations.
- I – Informed: Communication must occur into, out of, and across the committees and with campus.

Additional values include:

- Transparency: Governance structure and process must be clear. How decisions are made and how users communicate with ITSAC must be readily apparent to campus.
- Appropriate Representation: Constituency groups across campus must be represented.

The ITSAC membership includes the following members:

- The Chief Information Officer, chair
- Designee appointed by the Vice President for Finance and Administration
- Faculty designee appointed by the Vice President for Educational Services
- Technical dean or department chair designee appointed by the Vice President for Educational Services
- Institutional Research Director or designee appointed by the Vice President for Educational Services
- Professional staff designee appointed by the Dean for Student Services
- Classified staff designee appointed by the Dean for Student Services
- Designee appointed by the President
- The ITS Technical Director, non-voting, ex-officio
- The ITS Manager of Instructional Technology Services, non-voting, ex-officio

Members will serve a two-year term, with half the members replaced each year.

(Revised 3/2019 – MH)

Information Technology **Regulation 8200**

Appropriate Use

State Fair Community College shall provide computing and networking resources to the campus community of students, faculty, staff, and the public to support its educational mission. The computing and networking facilities are a College resource. Computers and networks can provide access to resources on and off campus, as well as the ability to communicate with other users worldwide. Such open access is a privilege, and requires that individual users act responsibly. Users shall respect the rights of other users, respect the integrity of the systems and related physical resources, and observe all relevant laws, regulations, and contractual obligations. Computing and networking resources shall always be used in compliance with all international, federal, state, and local laws.

This regulation applies to all users of SFCC and computing and technology resources including faculty, staff, students, guests, external individuals or organizations and individuals accessing external network services, such as the internet via College facilities.

Preserving the access to information resources is a community effort that requires each member to act responsibly and guard against abuses. Therefore, both the community as a whole and each individual user have an obligation to abide by the following standards of acceptable and ethical use:

- Use only those computing and information technology resources for which you have authorization.
- Use computing and information technology resources only for their intended purpose.
- Protect the access and integrity of computing and information technology resources.
- Abide by the applicable laws and college policies and respect copyrights and intellectual property rights of others, including the legal use of copyrighted software.
- Respect the privacy and personal rights of others.

Failure to comply with the appropriate use of these resources threatens the atmosphere for the sharing of information, the free exchange of ideas and the secure environment for creating and maintaining information property and subjects one to discipline. Any member of the College community found using information resources for unethical and unacceptable practices has violated this policy and is subject to disciplinary proceedings including the suspension of system privileges, expulsion from school, termination of employment, and/or legal action as may be appropriate.

SFCC reserves the right to limit or restrict the use of its computing and information technology resources based on institutional priorities and financial consideration, as well as when it is presented with evidence of a violation of College policies, contractual agreements, or state and federal laws.

Although members of the community have an expectation of privacy, if a user is suspected of violating this policy, his or her right to privacy may be superseded by the College's requirements to protect the integrity of information technology resources, the rights of all users and the property of the College. The College, thus, reserves the right to examine material stored on or transmitted though its facilities if there is cause to believe that the standards for acceptable and ethical use are being violated by a member of the college community.

User Responsibilities:

Use of College computing and information technology resources is granted based on acceptance of the following specific responsibilities:

- Use only those computing and information technology resources for which you have authorization.

  For example: it is a violation

  - to use resources you have not been specifically authorized to use
  - to use someone else's account and password or share your account and password with someone else o to access files, data or processes without authorization
  - to purposely look for or exploit security flaws to gain system or data access

- Use computing and information technology resources only for their intended purpose.

  For example: it is a violation

  - to send forged e-mail
  - to misuse Internet Relay Chat (IRC) software to allow users to hide their identity, or to interfere with other systems or users
  - to use electronic resources for harassment or stalking other individuals
  - to send bomb threats or "hoax messages"
  - to send chain letters
  - to intercept or monitor any network communications not intended for you
  - to use computing or network resources for advertising or other commercial purposes

- to attempt to circumvent security mechanisms
- to use privileged access for other than official duties
- to use former privileges after graduation, transfer or termination

• Protect the access and integrity of computing and information technology resources.

For example: it is a violation

- to release a virus or worm that damages or harms a system or network
- to prevent others from accessing an authorized service
- to send e-mail bombs that may cause problems and disrupt service for other users
- to attempt to deliberately degrade performance or deny service
- to corrupt or misuse information
- to alter or destroy information without authorization

• Abide by applicable laws and College policies and respect the copyrights and intellectual property rights of others, including the legal use of copyrighted software.

For example: it is a violation

- to make more copies of licensed software than the license allows
- to download, use or distribute pirated software
- to operate or participate in pyramid schemes
- to distribute pornography o to upload, download, distribute or possess pornography

• Respect the privacy and personal rights of others.

For example: it is a violation

- to tap a phone line or run a network sniffer without authorization
- to access or attempt to access another individual's password or data without explicit authorization
- to access or copy another user's electronic mail, data, programs, or other files without permission

System Administrator Responsibilities:

System administrators and providers of College computing and information technology resources have the additional responsibility of ensuring the integrity, confidentiality, and availability of the resources they are managing. Persons in these positions are granted significant trust to use their privileges appropriately for their intended purpose and only

when required to maintain the system. Any private information seen in carrying out these duties must be treated in the strictest confidence, unless it relates to a violation or the security of the system.

Security Caveat:

Be aware that although computing and information technology providers throughout the College are charged with preserving the integrity and security of resources, security sometimes can be breached through actions beyond their control. Users are therefore urged to take appropriate precautions such as safeguarding their account and password, taking full advantage of file security mechanisms, backing up critical data and promptly reporting any misuse or violations of the policy.

Violations:

Every member of the College community has an obligation to report suspected violations of the above guidelines or of the Information Technology Policies - 8000. Reports should be directed to the unit, department, school, or administrative area responsible for the particular system involved.

If a suspected violation involves a student, a judicial referral maybe made to the Vice President of Student Services. Incidents reported to the Dean will be handled through the College Code of Student Conduct.

If a suspected violation involves a staff or faculty member a referral will be made to the individual's supervisor.

Access

Computing and networking resources shall be provided for the educational, academic, and administrative purposes of the College. Some computer labs, networks, systems, and other resources shall be restricted to students who are enrolled in specific courses or programs or employees who have specific work assignments. Computer users shall learn and follow the access regulations for each resource used and shall use the resources appropriately and consistently with access regulations.

The use of these computers/networks is a privilege granted to members of the college community. When using this account, you are agreeing to:

1. Take no actions which violate the Information Technology Appropriate Use regulation 8200, Employee Handbook, or other applicable policy or law.
2. Use these resources only for purposes consistent with the College's mission and applicable policy or law. Inappropriate use includes, but is not limited to:
    a. sending harassing messages or in any way harassing other computer users;
    b. gaining OR attempting to gain access to accounts or files without permission on any computer or network system;
    c. making unauthorized copies of any copyright protected software, or other copyrighted or trademarked material, regardless of source;
    d. taking actions which threaten the security or capacity of computer or network systems, or which destroy, damage or overload these resources;
    e. violating any applicable law or policy.

Failure to abide by these policies will result in revocation of your privileges to use computing and network resources. Although we have backup procedures in place, use of these facilities is at your own risk since recoverability and security of data cannot be guaranteed. Files, data and disks may be considered SFCC property and are therefore subject to access by the College. Certain data may also be subject to access pursuant to Missouri Public Records statutes, via subpoena, or consistent with other state or federal law.

Regulation 8400

Information Technology

Data Security & Retention

Information systems contain data necessary to conduct business of the College. This policy establishes data security practices for the privacy of College employees, students, alumni, and donors.

Data is an institutional resource and must be protected from unauthorized change, destruction, or disclosure, whether accidental or intentional.

Staff who maintain data and handle computer-generated documents must:

- use data and data access only as required in the performance of their jobs, or
- disclose confidential College data to other staff only on a need-to-know basis, or
- exercise due care to protect data from unauthorized use, disclosure, alteration, or destruction, or
- utilize disk encryption software for all SFCC laptops, and for office PC and portable storage for Banner INB users, or
- follow established data processing practices when connected to the database -
    - including the following: do not leave workstations unattended after logging-in
    - do not write down or display the password near the workstation
    - do not disclose a login account and password to anyone, including ETS personnel

The Information Technology department, ETS, is responsible for:

- maintaining a network and computer system that provides safeguards against unauthorized access of these data, and
- maintaining software and hardware encryption software for the enterprise, and
- providing a custodial environment for the maintenance of the database. It is not the responsibility of ETS to disseminate data to anyone on or off campus. Within the guidelines of this policy, that responsibility belongs to the head of the department which maintains the desired data, and
- maintaining and identifying the following information classifications for all College data:
    - Unclassified. Information or documents which are available to the public.
    - Internal Use Only. Information or documents restricted for use within the College which related to the institution's business. Computer generated reports listing students, staff, financial data and telephone directories are primarily for internal use only. Documents and data of this kind need not be kept under lock and key although reasonable care should be made to keep it from public view. Precautions must be taken when these data are transferred to another individual or destroyed.

- Confidential. Sensitive data that would breach reasonable privacy expectations or data that could be detrimental to students, staff members or the College if improperly disclosed. These data are made available only to those individuals whose job responsibilities require such data. This kind of data when printed on paper must be kept under lock and key and carefully safeguarded. Precautions must be taken when these data are transferred to another individual or destroyed.

Selling or transferring of e-mail addresses, mailing labels, or other serial data by anyone to outside agencies or vendors is prohibited unless approved by the department head.

Retention

Educational technology Services does document the back-up and retention procedures and ensure that those policies procedures are followed consistently. The retention policy specifies the amount of time that a particular item of ESI can be recovered after it has been deleted but in no case shall it exceed 120 days for data, or 183 days for e-mail.

• Responsibilities

Educational Technology Services (IT)

The central IT organization at the College and at each College location will establish and publish retention schedules for any back-up and deleted Electronically Stored Data managed by those groups. This will include, but is not limited to, systems such as the central email servers and Banner.

Legal Custodians

The legal custodian of the information remains responsible for ensuring that Electronically Stored Data that constitutes a College record is handled appropriately. IT system administrators are NOT the legal custodians of information that may be contained in back-up or deleted files.

Non-central IT organizations

Administrative, academic and other divisions or departments that provide or manage central storage service for their users must document their back-up and retention policies or procedures.

- Media Destruction
  Departments must ensure that tapes or other forms of media scheduled for destruction are disposed of properly.
- Electronically Stored Data
  The specific retention periods for each type of Electronically Stored Data maintained by the Educational Technology Services are listed in the table below. This applies only to deleted data and not data stored for archive purposes.
- E-Mail Retention & Archiving
  All e-mail on the SFCC email system shall be automatically archived for 18 months (sliding window). This is within the requirements for archiving of electronic communications in the regulation set forth by the Missouri Secretary of State, Section 109, RSMo. This retention period, chosen by the college, retains emails in the system up to one academic year.

Type of Record	Description	Official Repository	Duration
Info Technology, communications	Employee E-Mail	Educational Technology Services	18 Months
Info Technology, data	File and Web	Educational Technology Services	120 days
Info Technology, data	Log files	Educational Technology Services	120 days
Info Technology, data	User files and databases	Educational Technology Services	120 days
Info Technology, communications	Phone call detail logs	Educational Technology Services	120 days
Info Technology, communications	Voicemail	Educational Technology Services	0 Days
Info Technology, communications	Instant Messaging	Educational Technology Services	0 Days

The College complies with applicable laws and regulations regarding the dissemination and protection of data that is confidential. In particular, it adheres to the Family Educational Rights and Privacy Act of 1974, otherwise known as the Buckley Amendment.

Enforcement:
Violations of any part of this policy may result in disciplinary action as prescribed by College policies and procedures.
(Revised 3/2019 - MH)

Hardware and Software Support

The College shall maintain a list of supported computer hardware and software. Purchases of products on the College's list will be supported by Educational Technology Services in terms of compatibility, installation, training, maintenance, troubleshooting, and upgrades. Educational Technology Services may decline to provide support for products not on the list. Faculty and staff who wish to purchase products for institutional use that are not on the College list may submit those products to the appropriate Educational Technology Services advisory committee for review and possible recommendation to the President, who shall review recommendations during the annual budgeting process.

The Vice President of Technology Services will approve all purchases of hardware and software. Educational Technology Services may decline to provide support for products not on the standards list. Faculty and staff who wish to purchase products for institutional use that are not on the College's standard list may submit justification for the non-standard product to the Educational Technology Services Advisory Committee for review and possible approval. Appeals to the ETS Advisory Committee decision may be appealed to the Executive Leadership Team.

Please go to the Standards web page for the up to date hardware standards.

Information Technology **Regulation 8700**

Electronic Communications

The College provides e-mail services for faculty and staff for use when engaging in activities related to College business. Incidental personal use that does not interfere with College operations generate incremental identifiable costs, saturate the data networks of the College, or negatively impact the individual's job performance is permitted. E-mail may not be used for commercial purposes or for personal financial gain. In addition, users shall accept and comply with the individual responsibilities relating to computer and information technology set forth in the SFCC Appropriate Use Policy and Regulation 8200.

This e-mail policy covers all uses of the College e-mail facilities. Any user of College email facilities consents to all provisions of this regulation and agrees to comply with all of the terms and conditions set forth herein, all other applicable College policies, regulations, and procedures, and with applicable local, state, and federal laws and regulations.

Users of College E-mail Facilities whose actions violate this policy or any other College policy or regulation may be subject to revocation or limitation of e-mail privileges as well as other disciplinary actions or may be referred to appropriate external authorities.

Access to E-mail:

SFCC provides College E-mail Facilities for legitimate College-related activities to faculty, students, staff, and other individuals and entities granted e-mail privileges at SFCC, as well as connections between on-campus electronic mail systems and external data networks. The use of College E-mail Facilities -- like the use of any other Collegeprovided resource and like any other College-related activity -- is subject to the normal requirements of legal and ethical behavior within the College community. Thus, legitimate use of College E-mail Facilities does not extend to whatever is technically possible.

SFCC E-mail Account:

Staff members with access to a College-owned computer on campus and faculty are required to activate their Official SFCC E-mail Account. Users are expected to read, and shall be presumed to have received and read, all official SFCC e-mail messages sent to their SFCC E-mail Accounts.

Individual academic and administrative units may choose to operate their own e-mail facilities as an alternative to the centrally available resources, but the use of any such facilities shall also be subject to this policy.

Acceptable Use:

State Fair Community College provides College E-mail Facilities for activities and associated administrative functions supporting its mission of learning, discovery, and engagement. Although modest personal use of College E-mail Facilities is allowed, College E-mail Facilities should be used for College-related educational and administrative purposes. Any use of College E-mail Facilities that interferes with College activities and functions or does not respect the image and reputation of SFCC is improper.

Policies and regulations that apply to other forms of communications at the College also apply to electronic mail (Reference Regulation 8200 - Appropriate Use). In addition, the following specific actions and uses of College E-mail Facilities are improper:

1. Concealment or misrepresentation of names or affiliations in e-mail messages.
2. Alteration of source or destination address of e-mail.
3. Use of e-mail for commercial or private business purposes that have not been approved.
4. Use of e-mail for organized political activity or political solicitation.
5. Use of e-mail to harass or threaten other individuals.
6. Use of e-mail that degrades or demeans other individuals.

Public Record and Privacy:

Any e-mail sent from users at State Fair Community College or residing on SFCC E-mail Facilities may a public and may be subject to disclosure.

SFCC does not monitor the content of electronic mail as a routine procedure. The College reserves the right to inspect, copy, store, or disclose the contents of electronic mail messages, but will do so only when it believes these actions are appropriate to: prevent or correct improper use of College E-Mail Facilities; ensure compliance with College policies, procedures, or regulations; satisfy a legal obligation; or ensure the proper operations of College E-mail facilities or the SFCC Data Network. Any SFCC administrator who believes such actions are necessary must first obtain the written approval of an appropriate administrative authority: a dean in the case of an academic unit, or a director in the case of an administrative unit.

Use of E-mail for SFCC Business:

The official SFCC e-mail account shall be considered an official means for communicating College business, and may in some cases be the sole means of communication. Users are expected to read, and shall be presumed to have received and read, all official SFCC e-mail messages sent to their official SFCC e-mail accounts. Because the contents of such e-mail are subject to laws governing public records, users will need to exercise judgment in sending content that may be deemed confidential. Furthermore, e-mail transmissions may not be secure, and contents that are expected to remain confidential should not be communicated via e-mail. Common examples of confidential contents include: student grades, personnel records, individual donor gift records, and data subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Family Educational Rights and Privacy Act (FERPA) regulations, and the Gramm Leach Bliley Act (GLBA).

Deans, vice presidents, and their appointees may send broad-based messages relating to College business without any prior approval. The author of any business messages, however, assumes responsibility for assuring that messages do not violate any College policies, regulations, or procedures. Disclaimers of confidentiality included in e-mail messages do not protect the sender if confidential information is shared or disclosed inappropriately.

Mobile Communications

Cellular telephones and cellular-based wireless communications devices can be an effective resource for campus employees in the performance of their job duties. For employees who spend considerable time outside of their assigned office area, or who must be accessible outside of scheduled or normal work hours, a cellular or mobile device can be a significant benefit. Based on job duties, certain employees may qualify to be provided a stipend to cover the business use of personal cell phones. The college provides access to e-mail and calendaring through Blackberry Enterprise enabled phones. Other phones are currently not supported for access to these services.

Due to the requirement to comply with IRS regulations regarding personal use of institutionally owned devices and the difficulty and time intensive manual labor required to identify, track and determine personal versus business use, the College will no longer provide cell phone service to individual employees. In short, it will be up to the individual employee to claim business use based on appropriate documentation of personally owned cell phones, either as a reimbursement from the College or as a business deduction on their personal tax return.

The level of institutional cost for cell phone service has rapidly increased over the past few years. To bring costs more into line with the level of institutional benefit, a stipend regulation for cost sharing has been adopted. This regulation assumes that for most employees the device will be used for both personal and business use.

Certain employees may qualify for the college to provide an institutional stipend to cover the presumed business use of personal cell phones and service. The stipend will be considered taxable income to the employee. The level of cash subsidy (stipend) will be determined by a person's job duties as it relates to cell phone use and access. Guidelines to categorize cellular use as mandatory, beneficial or incidental are determined by the department head. The stipend includes the cost of service plus equipment. The college will review and set the amounts to be provided for stipends and reimbursement on an annual basis. Institutional Stipend This regulation institutes an institutional stipend to cover presumed business use of personal cell phones for certain employees

Institutional Stipend

This regulation institutes an institutional stipend to cover presumed business use of personal cell phones for certain employees.

1. Employee responsibilities: The employee will purchase cellular phone service and equipment and assume responsibility for vendor terms and conditions. The employee is responsible for plan choices, service levels, calling areas, service and phone features, termination clauses, and payment terms and penalties. The employee is also responsible for the purchase, loss, damage, insurance, and/or replacement of phone equipment.

2. Guidelines to receive a stipend: Based on job duties as it relates to cell phones, three categories are identified to determine if the employee should be provided a stipend to offset the cost of a personal cell phone and service.
    a. Mandatory--the institution requires an employee to have a cell phone to fulfill job duties. The President upon recommendation from an area Vice President will approve qualifying employees in this category. Employees in this category have duties that require access by the college while away from the office or in off-hour situations. Service is required for "on-call" personnel to be contacted in the event of an emergency or service need. Service is provided for life or safety requirements.
    b. Beneficial--the use of a cell phone is not mandatory but is considered highly beneficial to an employee to fulfill job duties. An area Vice President will approve the stipend paid to employees in their area that qualify under this category. Service is provided so that an employee can work more efficiently, or that their working conditions require that they are away from traditional communications resources. Simple convenience is not sufficient to qualify for a monthly stipend.
    c. Incidental or occasional use – reimbursement for business use of a personal device would be allowed at a fixed rate for all others. This would be in the form of a business related reimbursement request instead of a monthly stipend.

3. Levels of stipend payment: There are many cell phone carriers with varying plans for phone equipment and service. The payment levels are intended to cover a presumed level of business use of personally owned service and equipment in keeping with institutional benefit. The regulation assumes that for most employees the device will be used for both personal and business use, therefore the overall costs are shared.
    a. Basic Use/Voice Service – this stipend level is intended to cover a portion of the employee's expense for monthly service costs and a contribution toward the cost of equipment and accessories. This stipend level would cover basic/voice cellular service to meet institutional job duties.

b. Enhanced Use/Voice + Data Service – this stipend level is intended to cover a portion of the employee's expense for monthly service costs and a contribution toward the cost of equipment and accessories. This stipend level would include voice service, plus data phone or Smartphone features that provide access to e-mail or web based services that would be required to meet institutional job duties. This service would apply to Coaches and managers.
c. Mandatory Use/Full Voice + Data Service – this stipend level is intended to cover a substantial portion of the employee's personal expense for monthly service costs, equipment and accessories. This stipend level would apply to members of the Executive Leadership Team and to approved directors.
d. Incidental/Occasional Use – this reimbursement level will be a "per-minute flat rate" with appropriate documentation provided by the employee.

Amounts listed in each category above will be reviewed and set annually by the Vice President for Finance, Administration and Human Resources and approved by the Executive Leadership Team. The stipend amounts will be listed on the annual **Cell Phone Stipend Agreement**. The reimbursement flat rate can be obtained from the Business Office.

4. Additional Regulation Guidelines:
   a. The stipend amount will be considered taxable income to the employee and added to their monthly paycheck. The stipend levels are set to provide for the additional tax burden an employee would incur.
   b. The department of an employee receiving a monthly stipend, or incidental use reimbursement will provide the appropriate budget funding.
   c. A **Cell Phone Stipend Agreement** will be completed by the employee and approved by the area Vice President or President. Updates or changes to cell phone service (phone numbers, voice/data vs. voice only, stipend amount, etc…) will be reported promptly to the employee's department head. The list of users by departments will be approved for renewal each year and reported to the area Vice President or President.
   d. If the employee resigns, is terminated, transfers departments, or no longer qualifies for an institutional stipend; the area Vice President will promptly notify the Business Office to discontinue the stipend payment.
   e. The employee's supervisor and area Vice President or President are responsible for an annual review of the business need for a cell phone stipend and whether the agreement should be continued.
   f. Exceptions: there may be rare circumstances where the stipend level must be adjusted due to extenuating conditions. The President upon recommendation from a Vice President will approve exceptions.
   g. Certain "departmental assigned phones" will be provided by the College.
   h. If the level of expense by the employee exceeds the stipend amounts received from the College, the employee could claim the overage (with sufficient IRS documentation) on their personal tax return.

Guidelines for Mobile Phone Use

1. Personal use – the stipend regulation assumes that the cell phone will be used for both personal and business calls. Since the stipend amount is taxable as income, the employee is not required to track business vs. personal use to report to the college.
2. Institutional benefit – the stipend agreement requires that the personally owned device is available for business access. An employee receiving a stipend must maintain active cell phone service. The employee agrees to carry the cell phone with them, keep it charged and in operational condition, and be accessible for business use as required by their department head or supervisor.
3. Appropriate use – the employee agrees to use the phone in ways consistent with college regulations 8200, 8300, 8400 and all applicable local, state or federal laws. Inappropriate and unlawful use of cell phone features, such as camera equipment, is prohibited.
4. Use of a cell phone while operating a vehicle – cell phones users must be aware of state and municipal laws regarding the use of phones while driving. The laws vary widely by location. In addition, use of phones while driving can cause hazardous distraction, especially in adverse weather, heavy traffic, or limited visibility conditions.
5. Wireless network - The College has provided wireless access to campus resources in three its four locations. The wireless network is accessible from wireless laptops, netbooks, Mac's and PC's that have current antivirus software and can run the Cisco Clean Access application. Since a phone cannot yet support these applications it is in the best interest of the college to not allow access to the wireless network with mobile phones or PDA's.
6. Campus resources – Access to college e-mail and calendaring services is only supported with a Blackberry phone that has been enabled to work in an enterprise environment. Regulations 8200, 8300 and 8400 apply when using a mobile device to access campus Resources.
7. Phone security – To help secure the data that could be stored on the phone it is important to password protect the Blackberry phone.
8. Loss or theft – Report loss or theft of phone within 24 hours.

Departmental Provided Mobile Phones

There are some circumstances where a "departmentally assigned cell phone" may be provided by the College that is not assigned to a specific individual. In these cases, the College will provide cell phone service and equipment.

1. Service and equipment procurement – Business Office will arrange for service and phone equipment as appropriate.
2. Monthly billing statements from the carrier – Business Office will process the carrier invoices for payment. The invoice breaks down the costs by individual telephone number including voice and data service plans, special features, plus any equipment that might have been purchased for that phone number. When new service is ordered Business Office requires a budget number from the responsible department to associate

with the new phone number.

3. Departmental bill back – Business Office allocates the full amount of each individual billing statement to the responsible departmental budget number on a monthly basis. These charges are submitted electronically and employees will not get additional paperwork or summaries other than what is available through the normal budget review process. However, budget managers may contact Business Office at any time to obtain additional copies of the detailed billing statements that have been billed to the department. In the event that billing errors are detected by Business Office, or reported to Business Office, the carrier representative is contacted to make adjustments in subsequent billing periods.
4. Usage tracking and review - It is the responsibility of the department to review monthly billing statements. Employees should confirm the usage charges and review any additional features or equipment included on the statement. (7-25-11)

Privacy Notification

The college will use reasonable efforts to maintain the privacy of users accessing its Web site and portal. As with all online services, however, SFCC cannot guarantee users of its Web site and portal absolute privacy over their use. In some cases, user information may be subject to disclosure under state or federal public record or freedom of information laws. Further, while the college has in place a variety of security measures to safeguard against illegal access of information obtained through its Web site and portal, the college cannot provide complete assurance against illegal access. Additionally, information obtained through the college's Web site and portal may be disclosed in the course of a civil or criminal investigation.

This policy informs you of the information that we may collect from you, what we do with it, to whom it may be disseminated, and how you can access it.

Network Traffic

In the course of ensuring network security and consistent service for all users, the college employs software programs to monitor network traffic, identify unauthorized access or access to nonpublic information and to detect computer viruses and other software that might damage college computers or the network. In the course of such monitoring, these programs may detect such information as e-mail headers, addresses from network packets and other information. Information from these activities is used only for the purpose of maintaining the security and performance of the college's networks and computer systems. Personally identifiable information from these activities is not released to external parties without your consent unless required by law.

Information Automatically Collected

When you browse through any Web site and portal, certain information about you can be collected. We automatically collect and temporarily store the following information about your visit:

- the date and time of your visit;
- IP address; • browser type, operating system and language;
- the pages you visited; and
- the address of the Web site from which you came.

We use this information for statistical purposes and to help us make our site more useful to visitors. This site makes no attempt to identify individual visitors from this information.

Cookies
Cookies are pieces of information stored by your Web browser on behalf of a Web site. Portions of our site may use cookies to carry data about your current session at the site from one Web page to the next. We do not forward cookies to any external parties. If you prefer not to receive cookies, you may turn them off in your browser, or may set your browser to ask you before accepting a new cookie.

Information Voluntarily Provided by You
We may collect voluntary information from you on our Web site or portal in a variety of ways: through surveys, online forms and e-mails, an authentication feature, and the use of electronic payment functionality. This information can be data that could reasonably be used to identify you, including your name, address, telephone number, e-mail address, Social Security number, birth date, bank account information, credit card information, or any combination of information that could be used to identify you.

Any Web site or other electronic means that conducts online research with human subjects are required to follow the provisions of the college's Institutional Review Board (IRB)

Web sites that collect individually identifiable information and provide services to children 12 and under may also be required to comply with provisions of the Children's Online Privacy Protection Act (COPPA).

Disclosure
We will not sell, exchange or otherwise distribute your personally identifiable information without your consent. Personal data may be released, however, pursuant to a request for such data in accordance with state or federal public record or freedom of information laws, or in the course of a civil or criminal investigation. Further, if you are a student at the college, any personal data released by the college shall be done in accordance with the federal Family and Educational Rights and Privacy Act (FERPA).

In addition, the information that you voluntarily submit will be disclosed only to SFCC employees or officials, or those under contract with SFCC, with a "need to know" for purposes of fulfilling their job responsibilities. The information may be used to answer your questions, respond to any requests for assistance, authenticate you for access to certain transactions and information, process and give you credit for any payment transactions, aid in the planning, design and development of the Web site, and fulfill the college's legal obligations.

Security
Because e-mail sent to the college is not encrypted, you should not send messages containing information that you consider highly sensitive to any address on this Web site.

We use standard security measures to ensure that information provided by you, including your personally identifiable information, is not lost, misused, altered, or unintentionally destroyed. We also use software to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage. Except for those grounds previously stated, no attempts are made to identify individual users or their usage habits. The transmission of registration IDs and passwords, personalization information, and payment information is encrypted.

Your Access
The college may maintain personal data you disclosed during your use of the Web site or portal. If you would like to review your personal data, please contact the college. Student data is maintained by the Student Services Office and employee data is maintained by the Human Resources Office.

External Links
Our Web site and portal have links to many other non-profit, educational, and governmental institutions, and in a few cases, private organizations. You are subject to those sites' Privacy Policy when you leave this site. Reference in the college's Web site or portal to any specific service, company, or organization does not constitute its endorsement or recommendation by State Fair Community College. SFCC is not responsible for the contents of any "off-site" Web page referenced from our server. (Approved 5/19/2008)