

## Guidelines Governing Access and Usage of Communication Technologies (*Pending Revision*)

---

### **INTRODUCTION**

The purpose of these guidelines is to provide users of STC electronic communications resources with basic knowledge and general guidance for the proper, fair, efficient, and effective use of those resources. These guidelines comply with existing STC policies and state of Texas standards. For issues not addressed by this document, refer to applicable STC policies or state of Texas standards.

### **DEFINITIONS**

These definitions apply to terms as they are used in the following guidelines.

College/Unit Policy Officer: A person with responsibility for issues having broad-based policy implication for students, faculty, and staff in the college/unit; Dean or similar position.

Education Records: Records specifically related to a student and maintained by an educational institution or a party acting on its behalf. The Family Educational Rights and Privacy Act of 1974 protect these records.

Electronic Communications: The use of computers and network systems in communicating or posting information or material by way of electronic mail, bulletin board systems, electronic facsimiles, chat rooms, instant messaging, Internet/WWW, LAN/WAN tools, or other such electronic tools.

Network Systems: Includes Local Area, Wide Area, and Internet-based voice, video, and data networks, switches, routers, and storage devices.

System or Network Administrator: A college employee responsible for managing the operation of operating system environments of computers or network systems, respectively.

College Computers and Network Systems (Computing Resources): Computers, networks, servers, and other similar devices that are administered by the College and for which the institution is responsible. Throughout these guidelines, the shortened term “computer resources” is used to mean College computers and network systems.

### **PRIVACY, CONFIDENTIALITY AND PUBLIC RECORDS**

South Texas College will make reasonable efforts to maintain the integrity and effective operation of its electronic communications systems, but users are advised that those systems should in no way be regarded as a secure medium for the communication of sensitive or confidential information. Because of the nature and technology of electronic communications, the College can assure neither the privacy of an individual user’s use of the College’s electronic communications resources nor the confidentiality of particular messages that may be created, transmitted, or received. Users should be aware that electronic communications could, depending on the technology, be forwarded,

intercepted, printed, modified, or stored by others. Furthermore, others may access electronic communications as authorized under STC policies. The electronic communications of employees may be subject to the Public Information Act in the same way that printed or typed letters and memos are. **Therefore, employees are strongly encouraged to consider any and every electronic communication they produce, send, or receive with STC resources as public and official communiqué in the execution of their official job duty.**

## — PERMISSIBLE USES OF ALL ELECTRONIC COMMUNICATIONS —

### **AUTHORIZED USERS**

Only College faculty, staff, and students and other persons who have received permission from the Vice President for Information Services and Planning or duly designated school authority are authorized users of the College's electronic communications systems and resources. Access to electronic communication is a privilege and certain responsibilities accompany that privilege.

### **PURPOSE OF USE**

The use of any College resources for electronic communications must be related to school business, including academic pursuits particular to any faculty member's academic discipline. The College provides these forms of electronic communication to employees at College expense for performing only their specified and assigned duties for the College. Users are expected to be ethical and responsible in their use, including making efficient use of College electronic communications resources, and are subject to the provisions of these guidelines and Board policy.

## — PROHIBITED USES OF ALL ELECTRONIC COMMUNICATIONS —

Prohibited uses include, but are not limited to:

- Sending copies of documents in violation of copyright laws.
- Inclusion of the work of others in electronic communications in violation of copyright laws.
- Interfering with the intended use or normal operation of the information resources or otherwise harming or damaging College systems.
- Interception or "opening" of electronic communications except as warranted by appropriate school authority and in the execution of College policy and delegated duty.
- Use of electronic communications to harass or intimidate others or to interfere with the ability of others to conduct College business. Also excluded are transmissions that are racist, hostile, sexist, pornographic, or obscene. The recipient may perceive an unwanted message as abusive, threatening, or harassing, especially if repeated. Such communication may be a breach of College policies and law.

- Using electronic communications to transfer material of a nature that would impede, interfere with, or otherwise diminish an employee's effectiveness at the College.
- Violating policy, rules, or other regulations while utilizing or accessing those systems through the school network.
- Using or knowingly allowing another to use any computer, computer network, computer system, program, or software to devise or execute any artifice or scheme to defraud or obtain money, property, services, or other things of value by false pretenses, false promises, or representations.
- Use of electronic communications systems for any purpose restricted or prohibited by laws or regulations.
- Constructing an electronic communication so it appears to be from someone else or otherwise adopting the identity of another person or affiliate on any electronic communication, using someone else's password, or sending electronic communications anonymously where anonymity is not granted or extended in the conduct of school business.
- Obtaining access to the files or electronic communications of others except as warranted by appropriate school authority and in the execution of College policy and delegated duty.
- Encryption devices are not allowed on college owned electronic resources.
- Attempting unauthorized access to electronic communications, attempting to breach any security measures on any electronic communication system, or attempting to intercept any electronic transmissions without proper authorization.

## — ACCESS AND DISCLOSURE —

### **GENERAL PROVISIONS**

The College reserves the right to access and disclose the contents of faculty, staff, students', and other users' electronic communications without the consent of the user. The College will do so when it believes it has a legitimate business need and only after explicit authorization is obtained from the Vice President for Information Services and Planning or duly designated school authority.

Faculty, staff, and other non-student users are advised that the College's electronic communications systems should be treated like a shared filing system, with the expectation that communications sent or received on College business or with the use of College resources may be made available for review by any authorized College official for purposes related to College business.

Electronic communications of students may constitute "education records" subject to the provisions of federal statute. The College may access, inspect, and disclose such records under conditions that are set forth in the statute.

### **INSPECTIONS AND DISCLOSURE OF COMMUNICATIONS**

South Texas College reserves the right to inspect and disclose the contents of electronic communications as needed to protect health and safety, to prevent

interference with the academic mission, to locate substantive information required for College business that is not more readily available by some other means, in the normal course of explicitly defined supervisory responsibilities, or in the course of an investigation triggered by indications of misconduct or misuse.

The College will inspect and disclose the contents of electronic communications when such action is necessary to respond to legal processes and to fulfill the College's obligations to third parties.

### **REPORTING PROHIBITED USES OF ELECTRONIC COMMUNICATION**

If you believe that a violation of these guidelines has occurred, contact the Office of ITS Client Services immediately. There may be situations when the following additional offices should be contacted:

- Office of the Director of Operations and/or Director of Security, if an individual's health or safety appears to be in jeopardy.
- Office of Human Resources, if violations occur in the course of employment.
- Office of the Vice President for Information Services and Planning, if an incident potentially bears external or legal consequences for the institution. You may also contact the VP of ITS if you wish to report an incident, but are unable to do so through normal channels.