

Rules and Regulations Governing Acceptable Use of Information Systems and Communication Resources

1. Introduction

The purpose of these Guidelines is to outline the acceptable use of information systems and communications resources and provide users of South Texas College (“the College”) with basic knowledge and general guidance for 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.

2. Overview

The intention of publishing Acceptable Use Guidelines at the College is not to impose restrictions that are contrary to the institutions established culture of openness, trust and integrity. The College endeavors to protecting employees, students and the institution from illegal or damaging actions by individuals, either knowingly or unknowingly.

Information Systems and communications resources, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, messaging systems, Internet/Intranet/Extranet-related systems and services, WWW browsing, electronic facsimile machines, and FTP, are the property of the College. These systems are to be used for school business in serving the interests of the institution, its faculty, staff and students in the course of normal operations.

Effective security is a team effort involving the participation and support of everyone at the College who deals with information and/or information systems. **It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.**

3. Purpose

The purpose of these guidelines is to outline acceptable use of information systems and communications resources at the College. These rules are in place to protect students, employees, and the College. Inappropriate use exposes the College to risks including virus attacks, compromise of network systems and services, and legal issues.

4. Scope

These guidelines apply to students, employees, contractors, consultants, temporaries, and other workers at the College, including all personnel affiliated with third parties. These guidelines apply to all equipment that is owned, operated, or leased by the College.

5. Guidelines

5.1. General Use and Ownership

1. While the College's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the institutions systems remains the property of the College. Because of the need to protect the College's resources, management cannot guarantee the confidentiality of information stored on any network device belonging to the College. The College assures neither privacy nor confidentiality of messages and communications created, transmitted or received through its systems. Therefore, all users should consider any and every electronic communications a potentially "public" document.
2. College **Policy 4712 Information Resources Security** requires that college-owned information resources be used only for official College purposes.
3. College **Policy 4713 Access to Information Systems and Electronic Communications** requires college administration to develop and enforce these regulations.
4. Only the Vice President for Information Services and Planning or duly designated school authority is authorized to grant access and privilege to the college's more restricted information resources, such as user accounts, messaging services, and network administration.
5. No required software program or information can be removed from any operating system, database, or file unless explicitly authorized in writing by IS&P and in conformance with the College's security policies, procedures, and standards. Additionally, software that bypasses, in any manner, approved security software or controls may not be written or installed. Required software will be deemed necessary by IS&P and will be installed on every new computer and server.
6. For security and network maintenance purposes, authorized individuals within the College may monitor equipment, systems, and network traffic at any time, per the Information Security Committee's **Network Audit Guidelines**.
7. The College reserves the right to audit networks and systems on a periodic basis to ensure compliance with these guidelines.

5.2. Security and Proprietary Information

1. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts, per the Information Security Committee's **Password Guidelines**.
2. All PC's, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less, or by locking (ctrl-alt-delete for Windows 2000 users) when the host will be unattended. Appropriate service packs, hot fixes, and updates will be kept up to date on every computer.
3. All servers should be secured in accordance to the Information Security Committee's **Server Security** and **Server Maintenance Guidelines**.
4. No one is allowed to attach any desktop computer, laptop, or other intelligent device onto the STC network without receiving proper

authorization from Client Services, in accordance with **Policy 4712 Information Resources Security**.

5. Postings by users from the College email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the College, unless posting is in the course of business duties. Contact Public Relations for sample disclaimers.
6. Anti-Virus procedures will follow the Information Security Committee's **Anti-Virus Guidelines**.
7. On termination of employment or a contractual relationship with the College, or as otherwise requested by appropriate management, personnel must surrender all property and information managed by the College, and must not subsequently disclose any confidential or sensitive information.

5.3 Incidental Usage Clause

It is permissible to use the college information system for incidental purposes. This does not include uses requiring substantial expenditures of time, uses for profit, or uses that would otherwise violate college policy with regard to employee time commitments or company equipment.

5.4 Unacceptable Use

The following activities are, in general, prohibited. Administrative and other authorized users may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is a person at the College authorized to engage in any activity that is illegal under local, state, or federal law while utilizing the College-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities that fall into the category of unacceptable use.

5.4.1 Systems and Network Activities

The following activities are strictly prohibited:

1. Violations of the rights of any person or institution protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the College.
2. Violations of any municipal, state, and/or federal laws pertaining to Information Technology (e.g. Miller v California, 1973, concerning Internet obscenity).

3. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the College does not have an active license is strictly prohibited.
4. Unauthorized access to a particular machine, folder, and/or file. Unauthorized access is defined as any person not having explicit permission via username to the particular machine, folder, and/or file. Unauthorized access can also be left to the discretion of the machine operator.
5. Interfering with the intended use or normal operation of the information resources, or otherwise harming or damaging college systems, knowingly or unknowingly.
6. Deliberately using electronic communications to transfer material of a nature that would seriously impede, interfere with, or otherwise diminish an employee's effectiveness at the College.
7. Employees should not transmit confidential information concerning students or others to unauthorized parties, and to use care to protect against negligent disclosure of such information.
8. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
9. Intentional introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
10. Revealing your personal account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
11. Violating policy, rules or other regulations imposed by outside or external information providers while utilizing or accessing those systems with College resources.
12. No person should represent that any personal views contained in any communication emanating from College equipment are those of the College.
13. Using the College computing asset to actively engage in procuring or transmitting material that is in violation of applicable sexual harassment or hostile workplace laws.
14. Making fraudulent offers of products, items, or services originating from any of the College accounts.
15. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
16. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the person is not an intended recipient or logging into a server or account that the person is not expressly authorized to access, unless these duties are within the scope of

- regular duties. For purposes of this section, “disruption” includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information.
17. Port scanning or security scanning is expressly prohibited unless prior notification to the Information Security Committee is made.
 18. Executing any form of network monitoring which will intercept data not intended for the person’s host, unless this activity is a part of the person’s normal job/duty.
 19. Circumventing user authentication or security of any host, network or account.
 20. Interfering with or denying service to any user other than the person’s host (for example, denial of service attacks).
 21. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user’s terminal session, via any means, locally or via the Internet/Intranet/Extranet.
 22. Personnel shall not disclose any confidential or sensitive information unless it is properly required in their jobs, or except as authorized in writing pursuant to security policies. Such information includes technical and business information, information systems and software development and products and software licenses disclosed on a confidential basis to the institution.

5.4.2 Email and Communication Activities

1. Sending unsolicited email messages, including the sending of “junk mail” or other advertising material to individuals who did not specifically request such material (email SPAM).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster’s account, with the intent to harass or to collect replies.
5. Creating or forwarding “chain letters”, “Ponzi” or other “pyramid” schemes of any type.
6. Use of unsolicited email originating from within the College’s networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by the College or connected via the College’s network.
7. Posting the same or similar non-college-related messages to large numbers of Usenet newsgroups (newsgroup SPAM).
8. Encryption devices which are not approved by IS&P will not be allowed on any electronic resources.

5.5 Enforcement

1. If you believe that a violation of these guidelines has occurred, contact the Office of IS&P Client Services immediately. Under no circumstances should the witness(es) attempt to look through or access the suspect's machine in order to conduct their own personal investigation. There may be situations when the following additional offices should be contacted:
 - Office of the Director of Operations and Maintenance and/or the campus 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 IS&P if you wish to report and incident but are unable to do so through normal channels.

Any person found to have violated these guidelines might be subject to disciplinary action, up to and including termination of employment or expulsion from school. In addition, there may be cases in which a person may be subject to civil or criminal liability.

5.6 Definitions

Term	Definition
<i>SPAM</i>	Unauthorized and unsolicited electronic mass mailings.

6 Revision History

6/4/03 – Removed the words “or end user” after the word “College” in paragraph 5.4.1.3.

6/07/06- Replaced ITS with IS&P