SOUTHEAST Technical College

Policies and Regulations

Policy STC 841.1

Instruction

Acceptable and Ethical Use of Technology Resources

Southeast Technical College Technology Resources

Technology Resources at STC include, but are not limited to, the following: network, Internet, computer hardware, application software, printers, servers, data files, stored text, electronic mail, local databases, externally accessed databases, CD/DVD ROM, optical media, clip art, digital images, digitized information, STC hosted web space, communications technologies, and any new technologies as they become available.

User Terms and Conditions

The use of STC's technology resources is subject to the following terms and conditions: The use of technology resources must be for educational and/or research purposes consistent with the mission, goals, and objectives of STC along with State and Federal regulations.

In compliance with federal law, STC shall operate a technology protection measure that blocks or filters Internet access. The technology protection measure shall protect against access by adults and minors to content that is abusive, obscene, profane, sexually explicit, threatening, illegal or pertains to pornography. STC shall make every effort to restrict access to inappropriate materials and shall monitor the online activities of the end users; however, it is impossible to control all materials on a global network. Therefore, STC shall not be liable for the content or viewing of any materials not prepared by STC. Faculty may file a request with the Network Administrator to unblock websites that they believe have significant educational value. If the website is determined to be appropriate, the site will be unblocked.

Disciplinary action may be taken against students whose on-site communication causes a substantial disruption to the education environment or interferes with another student's rights. Criminal action may be taken against students if their on-site communication constitutes a threat.

All user accounts are considered the property of STC. STC expressly reserves the right at any time to review the subject, content, and appropriateness of electronic communications or other computer files and remove them if warranted, reporting any violation to the school administration or law enforcement officials.

User accounts of STC graduates will remain active through one term following graduation.

Students who withdraw, terminate enrollment or are expelled will have their account disabled immediately.

Persons using the STC network shall have no expectation of privacy or confidentiality in the content of electronic communications or other computer files sent and received on the STC network, regardless of whether the equipment used is personal or STC provided. All persons using the STC Network regardless of whether the equipment used is personal or STC provided are governed by STC Policies/Regulations.

Prohibited technology resource activities include, but are not limited to, the following:

- Sending, accessing, uploading, downloading, or distributing offensive, profane, threatening, pornographic, obscene, or sexually explicit materials.
- Downloading or transmitting multi-player games, music, or non-educational video files using the school network.
- Vandalizing, damaging, or disabling property of the school or another individual or organization.
- Accessing another individual's material, information, or files without permission.
- Using the network or Internet, which also includes STC e-mail and/or web pages, to solicit sales or conduct business. Users shall not set up web pages to advertise or sell service.
- Releasing files, home address, personal phone numbers, user ID's, passwords, or other vital information.
- Violating copyright or other protected material laws without the express consent or authorization of the owner of the copyrights.
- Attempting to repair, remove, or install hardware components reserved for an authorized service technician.
- Subscribing to mailing lists, mass e-mail messages, games, or other services that cause excess traffic that can slow the system and waste other users' time and access.
- Users are responsible for all use of the network under their accounts, regardless of whether access is gained with or without the person's knowledge and/or consent. Immediately notify the IT Department if you suspect any unauthorized use of your account. The user shall remain liable and responsible for any unauthorized use until the STC Information Department is notified of the suspected unauthorized use and has reasonable opportunity to act upon such notice.
- Intentionally damaging equipment or software or intentionally attempting to harm or destroy data of another person. This includes, but is not limited to, "hacking" and the loading or creation of computer viruses. The user who is responsible for the incident will be held liable for damages or cost of correcting the problem.
- Attempting to log on to the Internet or network (servers, routers, switches, printers, firewall) as system administrator.

- Installing, enabling, launching, or creating programs that interfere with the performance of the network, Internet, or hardware technology resources.
- Attempting to defeat computer or network security.
- Use of proxy sites or other means to circumvent the STC filter.
- Attempting to or installing equipment on or making modifications to the STC network without pre-authorization from the STC's Director of Information Technology/CIO.

Consequences will vary depending on the severity of the infraction which could include, but is not limited to temporary suspension of access to STC Technology resources, referral to law enforcement authorities, and possible long term suspension or expulsion from STC.

STC does not guarantee that the network will be uninterrupted or error-free; nor does it make any warranty as to the results to be obtained from use of the service or the accuracy or quality of the information obtained on or by the network. Access to the network is provided on an "as is" basis without warranties of any kind. Neither STC nor any of its agents or employees shall be liable for any direct, indirect, incidental, special, or consequential damages arising out of the use of or inability to use the network or out of any breach of any warranty.

Security of the network at STC is a high priority. Anyone observing a security problem on the STC network shall notify STC personnel. Any person identified as a security risk or having a history of problems with other computer systems may be denied access to the STC network.

STC's network may not be used for personal gain, which includes STC email and/or web pages, to solicit sales or conduct business.

Ethical Use of STC, Public, or Private Technology Resources
Ethical behavior requires that STC staff and students show consideration and respect whenever using computers or electronic communication/technology/devices/resources. When interacting with each other, STC staff and students shall:

(a) not include in electronic communication between staff, students and/or parents/guardians, comments or content that would not be acceptable in a face-to-face communication;
(b) not disclose, use, or disseminate unauthorized personal information of another person;
(c) distinguish between personal social networking sites and professional social networking sites. Staff shall not invite or accept current STC students, except for the staff person's relatives, into any personal social networking sites; and
(d) evaluate all information for its accuracy, reliability, and authority.

Disciplinary action may be taken against staff or students whose off-site communication causes a substantial disruption to the education environment or substantially interferes

with another's rights. Criminal action may be taken if the off-site communication constitutes a threat.

RELATED POLICIES:

STC 709 – Code of Conduct
STC 930 - STC 930.1 – Student Discipline
STC 955 – Student Records

Regulation		Board Action		
new:	11-25-96	28664	(formerly IJNDC-R/STC	07-01-25)
revised:	01-11-99	29241		
revised:	09-11-00	29683		
revised:	08-13-01	29922		
revised:	08-12-02	33308		
revised:	05-24-04	33830		
revised:	05-29-07	34735		
revised:	06-22-09	35422		
revised:	09-14-09	35491		
revised:	03-28-11	36009		
revised:	10-28-13	36752		