



## STI Technology Resources Policy

### Technology Resources at Southeast Technical Institute (STI)

Technology resources at Southeast Technical Institute 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, STI hosted web space, communications technologies, and any new technologies as they become available.

### Regulations

The use of Southeast Technical Institute's technology resources is a privilege, not a right. The privilege of using the technology resources provided by STI is not transferable or extendible to people or groups outside STI without authorized permission from the Director of Information Technology/CIO or the President of STI. This privilege terminates when a student is no longer enrolled at Southeast Technical Institute. This policy is provided to make all users aware of the responsibilities associated with efficient, ethical, and lawful use of technology resources. If a person violates any of these provisions, privileges may be terminated, access to the STI network may be denied, and other appropriate disciplinary action shall be applied, according to the Southeast Technical Institute discipline policy.

### User Terms and Conditions

The use of Southeast Technical Institute'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 Southeast Technical Institute along with State and Federal regulations. In compliance with federal law, STI 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. STI 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, STI shall not be liable for the content or viewing of any materials not prepared by STI. Disciplinary action may be taken against students whose on-site or off-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 or off-site communication constitutes a threat.



## Information Technology Policy Manual

User accounts are considered the property of STI. STI 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 STI 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 Southeast Technical Institute's network shall have no expectation of privacy or confidentiality in the content of electronic communications or other computer files sent and received on the STI network.

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 STI 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 STI 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 STI filter.
- Attempting to or installing equipment on or making modifications to the STI network without pre-authorization from the Southeast Technical Institute'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 STI Technology resources, referral to law enforcement authorities, and possible long term suspension or expulsion from STI.

Southeast Technical Institute 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 STI 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 Southeast Technical Institute is a high priority. Anyone observing a security problem on the STI network should notify an instructor or the STI Information Technology Department personnel. Any person identified as a security risk or having a history of problems with other computer systems may be denied access to the STI network.

Users shall be responsible for any costs, fees, charges, or expenses incurred under the person's user account in connection with the use of the network except such costs, fees, charges, and expenses as STI explicitly agrees to pay.

### **Laptop Policies**

#### STI Laptop Conditional Sales Agreement

Apple Mac Book Pro's will only be distributed to students who are currently enrolled in Graphics Communications or Animation Technology programs. All other students (laptop included programs and non-laptop included programs) will use a PC laptop.



Laptops that have software or hardware that malfunctions or is damaged must be brought to the Southeast Technical Institute's Information Technology Department's Help Desk. STI will be responsible for repairing computer software or hardware malfunctions under warranty.

Laptops that are under warranty through STI must be brought to the STI Help Desk for warranty work. Any tampering or removal of laptop parts other than by a certified service technician will void all warranties.

Students who select to bring their own laptop are on their own. Technical support and program specific software are the responsibility of the student.

Laptops that are stolen must be reported immediately to the police department and to STI's Technology Department.

Laptops and accessories that are under contract with STI are to be brought to the STI Help Desk when a student graduates, withdraws, terminates enrollment, or is expelled. At that time software that is owned by STI and/or the school district will be removed from the student's laptop.

If a student fails to return the computer at the above mentioned times of departure the student will be charged and/or a hold will be placed on their account for any STI owned software applications that are not removed by the STI Help Desk. Upon the software removal, the system will be set back to factory settings, including software which was shipped with the system.

Laptops are serviced on a first come first serve basis, and warranty parts are delivered and installed as they are received within the vendor parts return policy.

### **Student-owned Laptops (non-purchased STI laptops)**

Students who bring their own laptop to campus will only have access to STI Public Wireless Network, which only gives them access to Internet connectivity. Access to all other campus resources i.e (printing and datacluster) will not be available through non-STI purchased laptops. To gain access to these campus resources, students must log in with their STI username and password on a computer on campus which is on the STI secured network. All computer labs and Public Kiosks on campus will be available to all students and are connected to the STI secured network.



## Information Technology Policy Manual

Students who access the STI Public Internet, must have one of the following active and up to date anti-virus programs.

Norton AntiVirus  
McAfee VirusScan Plus  
Tren Micro Internet Security  
AVG Anti-Virus

### Revision History

February 1, 2008	Policy effective date
March 1, 2009	Added STI Public Wireless Network info