

## **Use of STCC Information Technology Resources (Revised 2/28/11)**

This is the policy for students, faculty, staff (both full and part-time) and all other authorized individuals (“guests”) at Springfield Technical Community College (“STCC”) on the use of **STCC Information Technology Resources**, including computers, printers and other peripherals, programs, data, local and wide area networks, email, and the Internet. In addition to this policy, individual schools/departments may choose to issue additional policies governing the use of STCC Information Technology Resources. Use of STCC Information Technology Resources by any student, faculty, staff or guest (“Users”) shall constitute acceptance of the terms of this policy and any such additional policies.

### **User Responsibilities**

It is the responsibility of any person using STCC Information Technology Resources to read, understand, and follow this policy. In addition, Users are expected to exercise reasonable judgment in interpreting this policy and in making decisions about the use of Information Technology Resources. Any person with questions regarding the application or meaning of this policy should seek clarification from appropriate supervisors. Additionally, Users must comply with all applicable College policies and procedures and state and federal law. The use of STCC Information Technology Resources is a privilege, not a right, and failure to observe this policy may subject individuals to disciplinary action, including, but not limited to, loss of access rights, expulsion from the College and/or termination of employment. Further, failure to observe this policy may result in violation of civil and/or criminal laws.

### **Acceptable Uses of STCC Information Technology Resources**

STCC firmly believes that Information Technology Resources empower Users and make their education and work more fulfilling and successful. Acceptable use of STCC’s computing and networking resources includes usage for academic, educational or professional purposes which are directly related to official College business and in support of STCC’s mission. All students and guests must sign in legibly on appropriate logs each time they use the network.

### **Unacceptable Uses of STCC Information Technology Resources**

The following uses of STCC’s Information Technology Resources are unacceptable uses. This list of unacceptable uses is not exhaustive. It is unacceptable to use STCC Information Technology Resources:

- in furtherance of any illegal act, including violation of any criminal or civil laws or regulations, whether state or federal;
- for any political purpose not permitted under a collective bargaining agreement or contrary to any state or federal law;
- for any commercial purpose, including but not limited to soliciting the purchase, sale, rental or lease of private personal property, goods, services or real estate;
- to send threatening or harassing messages, whether sexual or otherwise;
- to access or share sexually explicit, obscene, or child pornography materials;
- to infringe any intellectual property rights;
- to gain, or attempt to gain, unauthorized access to any computer or network;
- or any use that causes interference with or disruption of network users and resources, including propagation of computer viruses or other harmful programs;
- to intercept communications intended for other persons;
- to share your password information with any other person;
- to misrepresent either STCC or a person’s role at STCC;

- to distribute chain letters;
- to access online games or gambling sites;
- to libel or otherwise defame any person;
- for any use that results in an unauthorized, non-college expense to the College (such as enrollment in phone messaging services);
- to consume excessive bandwidth and/ or storage as determined by STCC officials in their sole discretion; or
- to use STCC Information Technology Resources to violate the “Student Code of Conduct” as described in the Student Handbook or other College policies and procedures.

### **Data Confidentiality**

Users shall not access, release, use, or disseminate (via email or otherwise) confidential or proprietary information such as personal data about identifiable individuals (including unencrypted PAN or “Personal Account Numbers”) or commercial information about business organizations, unless the individual User is authorized by STCC to do so and such access, release, use, or dissemination is consistent with state and federal law. The confidentiality of student educational records shall additionally be subject to the requirements of the Family Educational Rights and Privacy Act (FERPA).

### **Copyright Protection**

Computer programs are valuable intellectual property. Software publishers can be very aggressive in protecting their property rights from infringement. Users are not permitted to use any software unless it is properly licensed to STCC. In addition to software, legal protections can also exist for any information published on the Internet, such as the text and graphics on a web site. As such, it is important that Users respect the rights of intellectual property owners. Users should exercise care and judgment when copying or distributing information that could reasonably be expected to be copyrighted. Pursuant to the Digital Millennium Copyright Act, 17 U.S.C. “1203(i)(1)(A), Users who engage in copyright infringement shall, at a minimum, have his/her access privileges terminated.

### **Computer Viruses**

Users should exercise reasonable precautions in order to prevent the introduction of a computer virus into the local area or wide area networks. Virus scanning software, approved by the IT Department, will be used at all times and, specifically, to scan storage media used to transport data such as floppy diskettes, CDs, flash drives, etc. The IT Department will install centrally managed antivirus client software configured to receive updates automatically on all College owned computers. In addition, executable files (such as program files that end in “.exe”) should not be stored on or run from network drives unless authorized, installed and maintained by the IT Department. Finally, it is a good practice to scan computer hard drives periodically to see if they have been infected. Please contact the IT Help Desk ([helpdesk@stcc.edu](mailto:helpdesk@stcc.edu) or 413-755-4016) with any questions.

### **Security**

Most desktop computers are connected to a local area network, which links computers within STCC and, through the wide area network, to the Internet. As such, it is critically important that Users take particular care to avoid compromising the security of the network. Users shall not connect any device to any STCC computer equipment or to the STCC campus network without the written permission and involvement of the IT Department. This includes, but is not limited to

servers, personal computers, notebook/laptop computers, printers, hubs, switches, routers, firewalls, wireless access points, etc.

Because the installation of unauthorized software can severely compromise computer and network security, Users are not permitted to install any software on STCC computers without the permission of management and the involvement of IT personnel. Under no circumstances will IT personnel be responsible for the installation and/or configuration of software or hardware on any non-STCC equipment.

Users must never share their passwords with anyone else, and should promptly notify the IT Help Desk (helpdesk@stcc.edu or 413-755-4016) if they suspect their passwords have been compromised. In addition, Users who will be leaving their PCs unattended for extended periods (more than 30 minutes) should either log off the network or have password-protected screen savers in operation. Finally, no User is allowed to access the Internet or other external networks via modem without written permission from management and the involvement of the IT Department. Users must notify the IT Help Desk (helpdesk@stcc.edu or 413-755-4016) if they identify a security issue.

### **E-Mail**

When using e-mail, there are several points Users should consider. E-mail addresses identify the organization that sent the message (Ex. EmployeeName@stcc.edu). Thus, Users should ensure that all e-mails are written in a professional and courteous tone. Furthermore, although many Users regard e-mail as offering a quick, informal way to communicate, Users should remember that e-mails can be stored, copied, printed, or forwarded by recipients. As such, Users should not write anything in an e-mail message that they would not feel just as comfortable putting into a formal memorandum.

### **College use of email**

Email is considered an official method of communication. Official email communications are intended to meet the academic and administrative needs of the campus community. The College has the right to expect that such communications will be received and read in a timely fashion. To enable this process, the College ensures that all students in credit-bearing courses can access a standardized, college-issued email account throughout their academic years at STCC.

### **Expectations about student use of email**

Students are expected to check their STCC official email on a frequent and consistent basis in order to remain informed of College related communications. Checking email on a daily basis is recommended. (There are many computer stations and labs placed around campus for free student use, such as in the Student Success Center, Building 27, 1st floor). Students have the responsibility to recognize that certain communications may be time-critical. 'I didn't check my email' or 'my mailbox was full' are not acceptable excuses for missing official College communications via email.

### **Appropriate use of student email**

Users should exercise extreme caution in using email to communicate confidential or sensitive matters, and should not assume that email is private and confidential. It is especially important that users are careful to send messages only to the intended recipient(s), especially when using the 'reply' command during email correspondence. Finally, although many users regard e-mail as being like a telephone in offering a quick, informal way to communicate, users should

remember that e-mails can be stored, copied, printed, or forwarded by recipients. As such, users should not write anything in an e-mail message that they would not feel just as comfortable putting into a memorandum.

### **Educational uses of email**

Faculty will determine how email will be used in their classes. This ‘Official Student Email Policy’ will ensure that all students will have the tools to comply with email-based course requirements from the faculty. Faculty can, therefore, make the assumption that students’ official @student.stcc.edu accounts are being accessed by their student. All use of email will be consistent with other College policies.

### **Social Media**

The use of all STCC Information Technology Resources, including but not limited to Facebook, YouTube, Twitter, blogs or other forms of social media, shall be limited to academic, educational, or professional purposes, which are directly related to official College business and in support of the College’s mission. All such uses shall comply with other sections of this Policy. Information Technology resources provided by the College are the property of the College; users shall have no expectation of privacy when using such resources.

### **No Expectation of Privacy**

STCC Information Technology Resources are the property of Springfield Technical Community College or the Commonwealth of Massachusetts and are to be used in conformance with this policy. When reasonable and in pursuit of legitimate needs for supervision, control, and the efficient and proper operation of the workplace, STCC will exercise the right to inspect any User’s computer, any data contained in it, and any data sent or received by that computer. Use of STCC Information Technology Resources constitutes express consent for STCC to monitor and/or inspect any data that Users create or receive, any messages they send or receive, and any web sites that they access, as well as monitor network activity in any form that STCC sees fit to maintain the integrity of the network. Therefore, Users shall have no expectation of privacy over any communication, transmission or work performed using STCC Information Technology Resources.

### **No Warranties**

STCC makes no warranties of any kind, whether express or implied, for the service it is providing. STCC will not be responsible for any damages a User suffers. This includes loss of data resulting from delays, no-deliveries, or service interruptions caused by STCC negligence or by the User’s errors or omissions. Use of any information obtained via the Internet is at the User’s own risk. STCC specifically denies any responsibility for the accuracy or quality of information obtained through its services. Users need to consider the source of any information they obtain and consider how valid that information may be.

STCC also specifically denies any responsibility for a User’s encounter, access or use of any inappropriate or controversial materials from STCC Information Technology Resources, including the Internet. Users must notify the IT Help Desk (helpdesk@stcc.edu or 413-755-4016) if they identify Information Technology Resources being used in a manner inconsistent with this Policy.