Operations Policy #915
Acceptable Usage Policy

Background:
Users will have access to school systems only after agreeing to the Acceptable Usage Policy. This policy covers school provided computers, internet access, networks and any other devices that are provided for use by the school such as printers, mobile devices, calculators or fitness devices. Violation of this agreement may lead to disciplinary action.

Purpose:
The goal of the SCCS, in providing school system access to staff and students, is to promote educational excellence in the school by facilitating resource sharing, innovation, creativity and communication. With this access comes the responsibility on behalf of the user to abide by the Acceptable Usage Policy and maintain a level of conduct as expected in an educational environment. The pitfalls associated with using technology in the educational setting can be successfully avoided when all end users adhere to strict guidelines. It is the charter school's intent to provide access to these resources in a safe and secure manner consistent with its educational goals. This policy serves to address these responsibilities and guidelines.

Definitions:
SCCS Network: All necessary components that affect the network's operation, including but not limited to computers, copper and fiber cabling, wireless communications and links, equipment closets and enclosures, network electronics, telephone lines, printers and other peripherals, storage media, and other computers and/or networks to which the SCCS network may be connected, such as the Internet or those of other institutions.

- E-mail: Electronic mail. Mail composed and transmitted on a computer system or network.
- Hardware: The physical components of a computer system-the computer, plotters, printers, terminals, digitizers, keyboards, mice, and so on.
- Internet (Web): A network of servers linked together by a common protocol, allowing access to millions of hypertext resources. It is also known as www., W3, and the World Wide Web.
- Software: Written coded commands that tell a computer what tasks to perform. For example, Word, PhotoShop, Excel, and Access are all software programs.

Users: Any one person who may have access to the SCCS network. This may include, but is not limited to administrators, guests, school board members, students, support staff, and teachers.

The System Administrator is an individual charged with the responsibility of supervising computing resources through which Internet access may be gained.

Internet Acceptable Usage Terms and Conditions:

- The purpose of accessing the SCCS Network and/or the Internet is to support education by providing access to unique resources and the opportunity for collaborative work. The use of an account must be in support of education, academic research, and consistent with the educational objectives of the school. Use of other organizations' networks or computing resources, must comply with the rules appropriate for that network and is the responsibility of the user using that network or computer resource. Transmission of any material in violation of any U.S. or state regulation is prohibited. This includes, but is not limited to: copyrighted, threatening, obscene, or pornographic material, or material protected by trade secret or property law.
- Use for product advertisement, for-profit purposes or political lobbying is generally not consistent with the purposes, goals, and ideals of the school. Illegal activities are strictly prohibited. Hate mail, harassment, discriminatory remarks, and other antisocial communications on the SCCS Network or Internet are prohibited.
- The use of the SCCS Network and/or Internet is a privilege, and inappropriate use can result in the cancellation of those privileges. Based upon the acceptable use guidelines outlined in this policy, the System Administrator(s) will deem what is inappropriate use of the SCCS Network and/or Internet Access and may take appropriate action. The System Administrator(s) and the CEO may suspend or close an account at any time as required. They must notify the user and, if appropriate, the parent/guardian in writing within two weeks of the reason for suspension or termination of an account. The administration, faculty, and staff of the school may also request the System Administrator(s) to deny, revoke, or suspend specific user accounts. Students and employees whose accounts are denied, suspended or revoked may appeal that decision through existing school policies and procedures.

Hardware and Software:

Users are expected to abide by the rules of the "Software and Hardware" section of this policy.

- SCCS computers are configured and maintained for educational and administrative purposes only and should not be viewed as the personal equipment of the user; therefore, the right is reserved to restrict configuration and installation of software and hardware on all school computers.
- Any software installed on SCCS computers must be licensed in accordance with the law. A separate license must be purchased for each computer upon which the software is installed. A copy of all licenses must be forwarded to technology department staff before installation.
- Users may not make unauthorized copies of copyrighted software.
- Users may not install any unauthorized games, programs, files, or other electronic media on school computers.
- Users may not move or remove equipment or install/configure hardware or software without authorization by technology department staff.
- Users may not physically damage or destroy hardware, alter or destroy data of another user, harm or destroy data on the network and/or the Internet by the introduction of worms or viruses, or any other networks that are connected to the SCCS network structure. Vandalism, including theft of computer components, will result in monetary damages paid by the perpetrator, as well as disciplinary action according to school policy.

Email:

- SCCS e-mail is to be used for educational purposes or school-related business.
- SCCS e-mail is not to be used for personal advertisement or business, or to forward chain letters or other mass mailings that are not school related.
- Users may not repost a message that was sent to them privately without the permission of the person who sent them the message.
- Excess e-mail or files taking up an inordinate amount of fileserver disk space may be removed by system administrators, after a reasonable time and after notification to the user.
- Users may not post private information about another person.
- Network users have no privacy expectation in their e-mail messages. The school may intercept or access stored communication at any time for any reason.
- Users may not use vulgar, abusive, profane or other offensive language in SCCS e-mail.
- Users may not discuss illegal activities on SCCS e-mail.

Password Policy:

- User passwords must be changed at a minimum of once every 90 days
- Passwords must consist of at least 8 characters with a combination of letters, numbers and special characters.
- Passwords must consist of at least one capital letter, one lower case letter, and one number.
- Passwords must not be shared with any other user. Student passwords are kept on record and are issued annually.
- In the event that a password may have been compromised, contact technology services so that a new password can be issued.
- When changing passwords, users are unable to utilize any of the 5 previously used passwords for that account.

Rights:

- The SusQ-Cyber Charter School reserves the right to log SCCS Network and Internet use, and to monitor fileserver space utilization by users, while respecting the privacy right of both school users and other outside users. The school reserves the right to remove a user account from the network to prevent further unauthorized or illegal activities. Authorized staff members are permitted to view student home directories that are stored on the SCCS network.

- All data on the SusQ-Cyber Charter School's servers, PCs, laptops, or network is considered property of the SusQ-Cyber Charter School and can be accessed at any time necessary by the system administrator(s) and CEO.

Etiquette:

- The user is expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:
- Be polite. Do not write or send abusive or offensive messages to others, including hate mail or antisocial communications.
- Use appropriate language. Do not swear, use vulgarities, or inappropriate language.
- Do not reveal your personal address or phone number or those of student colleagues, teachers, and staff.
- Note that electronic mail (e-mail) is guaranteed to not be private. People who operate the system do have access to all mail. Messages relating to, or in support of illegal activities, will be reported to the appropriate authorities. Users and their access may be monitored at any time. Prior consent of the user need not be obtained for such monitoring.
- Do not use the SCCS Network and/or Internet in such a way that you would disrupt the use of the network by other users.
- All communications and information accessible via the SCCS Network and/or Internet should not be assumed to be private property.

Disclaimer:

- The SusQ-Cyber Charter School makes no warranties of any kind, whether expressed or implied for the service it is providing. The school will not be responsible for any damages that a user may suffer. This includes loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions caused by its own negligence or user errors or omissions. Use of any information obtained via the SCCS Network and/or Internet is at the user's own risk. The school specifically denies any responsibility for accuracy or quality of information obtained through its services.
- All terms and conditions as stated in this document are applicable to the SCCS Network and Internet Accesses provided by the Cyber School. These terms and conditions shall be governed and interpreted in accordance with all Pennsylvania and federal laws and regulations, as well as all CIPA requirements.

Security:

- Security on any computer system is a high priority, especially when the system involves many users. If a user feels that he/she can identify a security problem through either the SCCS Network and/or Internet Access, the user must notify a System Administrator(s) or the CEO immediately. Do not demonstrate the problem to others. Do not use another individual's account without written permission from that individual. Do not give your password to any other individual. Attempts to log in to the system as any user other than yourself may result in cancellation of user privileges. Attempts to login to either the Network and/or Internet as a System Administrator will result in immediate cancellation of the user's privileges. Any user identified as a security risk, or having a history of problems with other computer systems will be denied access to the SCCS Network and/or Internet.

- Use of an Internet proxy is a violation of the security policy as it is a direct attempt to circumvent Internet filters. Any student or staff member that is found using any method of circumvention will be contacted and recommended for disciplinary action. Access to network resources and the Internet can be limited so access will be restricted to only vital websites and systems.

Vandalism:

- Vandalism will result in cancellation of privileges. Vandalism is defined as, but not limited to, the following: any attempt to alter or destroy data of another user; any attempt to harm or destroy data on the Network and/or Internet, or any other networks that are connected to the SCCS Network structure. This includes, but is not limited to, the uploading or creation of computer viruses, or the intentional misuse or vandalism of software or hardware.

Vendor Access:

- As Software as a Service or "SaaS" becomes increasingly popular, additional precautions need to be enforced due to the nature of the information stored on offsite systems. Vendors with access to personal information for SusQ-Cyber Charter School's students and staff must maintain documentation regarding the reason for access, the date and time and the school user that has authorized access. Vendor access to the information stored on remote servers must be granted based on a request for service by an authorized party.

TO THE EXTENT THAT ANYTHING IN THIS POLICY COULD BE CONSTRUED TO CONFLICT WITH APPLICABLE STATE AND/OR FEDERAL LAWS, THE APPLICABLE STATE AND/OR FEDERAL LAWS CONTROL. THIS POLICY IS NOT INTENDED TO CONFLICT WITH CHARTER REQUIREMENT.

Adopted 10/23/2012