SUN AREA TECHNICAL INSTITUTE

SECTION: OPERATIONS

TITLE: ACCEPTABLE USE OF COMPUTERS/INTERNET

ADOPTED: December 19, 2002

REVISED: February 18, 2010

815. ACCEPTABLE USE OF COMPUTERS/INTERNET

1. Purpose	The Joint Operating Committee supports use of the Internet and other computer networks in the center's instructional and operational programs in order to facilitate learning, teaching and daily operations through interpersonal communications and access to information, research and collaboration. The use of network facilities shall be consistent with the curriculum adopted by the center as well as the varied instructional needs, learning styles, abilities, and developmental levels of students.
2. Authority	The electronic information available to students and staff does not imply endorsement by the center of the content, nor does the center guarantee the accuracy of information received. The center shall not be responsible for any information that may be lost, damaged or unavailable when using the network or for any information that is retrieved via the Internet. The center shall not be responsible for any unauthorized charges or fees resulting from access to the Internet. The center reserves the right to log network use and to monitor fileserver space utilization by center users, while respecting the privacy right of both center users and outside users. The Joint Operating Committee establishes that use of the Internet is a privilege, not a right; inappropriate, unauthorized and illegal use will result in cancellation of those privileges and appropriate disciplinary action.
47 U.S.C. Sec. 254	The Joint Operating Committee shall establish a list of materials, in addition to those stated in law, that are inappropriate for access by minors.
3. Delegation of Responsibility	The center shall make every effort to ensure that this resource is used responsibly by students and staff.

	Administrators, teachers and staff have a professional responsibility to work together to help students develop the intellectual skills necessary to discriminate among information sources, to identify information appropriate to their age and developmental levels, and to evaluate and use the information to meet their educational goals. Students and staff have the responsibility to respect and protect the work of every other user in the center and on the Internet. The Administrative Director shall have the authority to determine what is inappropriate use.
20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254	The Administrative Director or designee shall be responsible for recommending technology and developing procedures used to determine whether the center's computers are being used for purposes prohibited by law or for accessing sexually explicit materials. The procedure shall include but not be limited to: 1. Utilizing a technology protection measure that blocks or filters Internet access for minors and adults to certain visual depictions that are obscene, child pornography, harmful to minors with respect to use by minors, or determined inappropriate for use by minors by the Joint Operating Committee. 2. Maintaining and securing a usage log. 3. Monitoring online activities of minors.
4. Guidelines	Network accounts shall be used only by the authorized owner of the account for its authorized purpose. All communications and information accessible via the network should be assumed to be private property and shall not be disclosed. Network users shall respect the privacy of other users on the system. <u>Prohibitions</u> Students and staff are expected to act in a responsible, ethical and legal manner in accordance with Joint Operating Committee policy, accepted rules of network etiquette, and federal and state law. Specifically, the following uses are prohibited: 1. Facilitating illegal activity. 2. Commercial or for-profit purposes. 3. Nonwork or nonschool related work.

	4. Product advertisement or political lobbying.
SC 1303.1-A Pol. 249	5. Bullying/Cyberbullying.
	6. Hate mail, discriminatory remarks, and offensive or inflammatory communication.
	7. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials.
Pol. 237	8. Access to materials, images or photographs that are obscene, pornographic, lewd or otherwise illegal.
	9. Access by students and minors to material that is harmful to minors or is determined inappropriate for minors in accordance with Joint Operating Committee policy.
	10. Inappropriate language or profanity.
	11. Transmission of material likely to be offensive or objectionable to recipients.
	12. Intentional obtaining or modifying of files, passwords, and data belonging to other users.
	13. Impersonation of another user, anonymity, and pseudonyms.
	14. Fraudulent copying, communications, or modification of materials in violation of copyright laws.
	15. Loading or using of unauthorized games, programs, files, or other electronic media.
	16. Disruption of the work of other users.
	17. Destruction, modification, abuse or unauthorized access to network hardware, software and files.
	18. Quoting of personal communications in a public forum without the original author's prior consent.

	Security System security is protected through the use of passwords. Failure to adequately protect or update passwords could result in unauthorized access to personal or center files. To protect the integrity of the system, the following guidelines shall be followed: 1. Employees and students shall not reveal their passwords to another individual. 2. Users are not to use a computer that has been logged in under another student's or employee's name. 3. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the network. Web 2.0 (Interactive Web Site Access)
47 U.S.C. Sec. 254 Pol. 218	Users may have access to Web 2.0 (interactive) web applications and other future/emerging technologies, such as, but not limited to, blogs, wikis, podcasts, social networking, social bookmarking, chats and message boards for purposes of instruction related to the curriculum. Users will access these sites for use as instructional tools only. Users will be directed to sites that utilize educational materials. Due to the nature of interactive web sites, access to these sites may result in exposure to inappropriate material that is not accessible to the Internet filter. Misuse of these sites may result in disciplinary action and could impact academic success. Classroom teachers will be responsible for monitoring and reporting abuses. Access to an interactive web site will be blocked if it is in violation of the Children's Internet Protection Act or any other local, state, or federal law with respect to the use of the Internet by minors. E-mail District employees may be provided with district e-mail accounts to use for educational purposes and district-related business. Students may be provided with district e-mail accounts to use for educational purposes. The following guidelines shall be followed: 1. Students are not authorized to access their personal e-mail accounts. 2. Users will not use e-mail for personal advertisements or to forward jokes, chain letters, or other mass mailings that are not school-related or appear to be spam.

	3. Users may not post any inappropriate material or material that could be constructed as harassment, libel or a threat of any sort. 4. Users may not use vulgar, abusive, profane or other offensive language on district e-mail.
Pol. 249	5. Users may not engage in bullying/cyberbullying. 6. E-mail for all district employees will be archived for a period of seven (7) years. Student e-mail will be archived while they are a student enrolled at the school. 7. Authorities may subpoena e-mail in the incidence of a legal action. <u>Consequences For Inappropriate Use</u> The network user shall be responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts. Illegal use of the network; intentional deletion or damage to files of data belonging to others; copyright violations; and theft of services will be reported to the appropriate legal authorities for possible prosecution. Under Pennsylvania law it is a felony punishable by fine of up to $15,000 and imprisonment of up to seven (7) years for any person to access, alter, or damage any computer system, networking, software or database, or any part thereof, with the intent to interrupt the normal functioning of an organization. Disclosing a password to a computer system, network, etc., is a misdemeanor punishable by a fine of up to $10,000 and imprisonment of up to five (5) years, as is intentional and unauthorized access to a computer or alteration of computer software. General rules for behavior and communications apply when using the Internet, in addition to the stipulations of this policy. Loss of access and other disciplinary actions shall be consequences for inappropriate use. Vandalism will result in cancellation of access privileges and legal prosecution. **Vandalism** is defined as any malicious attempt to harm or destroy data of another user, Internet or other networks; this includes but is not limited to uploading or creating computer viruses. <u>Copyright</u>
Pol. 814	The illegal use of copyrighted software by students and staff is prohibited. Any data uploaded to or downloaded from the network shall be subject to fair use guidelines.

	Safety To the greatest extent possible, users of the network will be protected from harassment and unwanted or unsolicited communication. Any network user who receives threatening or unwelcome communications shall report such immediately to a teacher or administrator. Network users shall not reveal personal information to other users on the network, including chat rooms, e-mail, Internet, etc.
20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254	Any center computer/server utilized by students and staff shall be equipped with Internet blocking/filtering software.
47 U.S.C. Sec. 254	Internet safety measures shall effectively address the following: 1. Control of access by minors to inappropriate matter on the Internet and World Wide Web. 2. Safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications. 3. Prevention of unauthorized online access by minors, including "hacking" and other unlawful activities. 4. Unauthorized disclosure, use, and dissemination of personal information regarding minors. 5. Restriction of minors' access to materials harmful to them.
	References: School Code – 24 P.S. Sec. 1303.1-A Child Internet Protection Act – 24 P.S. Sec. 4601 et seq. Enhancing Education Through Technology Act of 2001 – 20 U.S.C. Sec. 6777 Internet Safety – 47 U.S.C. Sec. 254 Joint Operating Committee Policy – 218, 237, 249, 814