VENANGO TECHNOLOGY CENTER

SECTION: OPERATIONS

TITLE: ACCEPTABLE USE OF INTERNET, COMPUTERS AND NETWORK RESOURCES

ADOPTED: June 1, 2009

REVISED: April 2, 2012

815. ACCEPTABLE USE OF INTERNET, COMPUTERS AND NETWORK RESOURCES

1. Purpose

The Joint Operating Committee supports use of the computers, Internet and other network resources 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 center provides students, staff and other authorized individuals with access to the center's computers, electronic communication systems and network, which includes Internet access, whether wired or wireless, **virtual, cloud** or by any other means.

The center intends to strictly protect its computer systems software and hardware against numerous outside and internal risks and vulnerabilities. Users are important and critical players in protecting these center assets and in lessening the risks that can destroy these important and critical assets. Consequently, users are required to fully comply with this policy and to immediately report any violations or suspicious activities to the director and/or designee. Conduct otherwise will result in actions further described in the Consequences for Inappropriate, Unauthorized and Illegal Use section found in this policy, and provided in other relevant school center policies.

For instructional purposes, 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. Definitions

The term child pornography is defined under both federal and state law.

18 U.S.C. Sec. 2256

Child pornography - under federal law, is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where:

1. The production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;

	2. Such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or 3. Such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.
18 Pa. C.S.A. Sec. 6312	Child pornography - under state law, is any book, magazine, pamphlet, slide, photograph, film, videotape, computer depiction or other material depicting a child under the age of eighteen (18) years engaging in a prohibited sexual act or in the simulation of such act. The term harmful to minors is defined under both federal and state law.
20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254	Harmful to minors - under federal law, is any picture, image, graphic image file or other visual depiction that: 1. Taken as a whole, with respect to minors, appeals to a prurient interest in nudity, sex or excretion; 2. Depicts, describes or represents in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or lewd exhibition of the genitals; and 3. Taken as a whole lacks serious literary, artistic, political or scientific value as to minors.
18 Pa. C.S.A. Sec. 5903	Harmful to minors - under state law, is any depiction or representation in whatever form, of nudity, sexual conduct, sexual excitement, or sadomasochistic abuse, when it: 1. Predominantly appeals to the prurient, shameful, or morbid interest of minors; 2. Is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable for minors; and 3. Taken as a whole lacks serious literary, artistic, political, educational or scientific value for minors.
18 Pa. C.S.A. Sec. 5903	Obscene - any material or performance, if: 1. The average person applying contemporary community standards would find that the subject matter taken as a whole appeals to the prurient interest;

	2. The subject matter depicts or describes in a patently offensive way, sexual conduct described in the law to be obscene; and 3. The subject matter, taken as a whole, lacks serious literary, artistic, political, educational or scientific value.
47 U.S.C. Sec. 254	Technology protection measure - a specific technology that blocks or filters Internet access to visual depictions that are obscene, child pornography or harmful to minors.
18 U.S.C. Sec. 2256(6) 20 U.S.C. Sec. 6777(e) Pol. 237	**Computer - includes any center owned, leased or licensed or User-owned personal hardware, software, or other technology used on center premises or at center events, or connected to the center network, containing center programs or center or student data (including images, files, and other information) attached or connected to, installed in, or otherwise used in connection with a Computer. For example, Computer includes, but is not limited to, the center and Users': desktop, notebook, powerbook, tablet PC or laptop Computers, printers, facsimile machine, cables, modems, and other peripherals, specialized electronic equipment used for students' special educational purposes, Global Position System (GPS) equipment, RFID, personal digital assistants ("PDAs"), iPods, MP3 players, thumb drives, cell phones (with or without Internet access and/or recording and/or camera/video and other capabilities), telephones, mobile phones or wireless devices, two-way radios/telephones, beepers, paging devices, laser pointers and attachments, Pulse Pens, and any other such technology developed.**
3. Authority	The availability of access to electronic information 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 or other network resources.
Pol. 218, 233, 317	The Joint Operating Committee declares that computer and network use is a privilege, not a right. The center's computer and network resources are the property of the center. Users shall have no expectation of privacy in anything they create, store, send, receive or display on or over the center's Internet, computers or network resources, including personal files or any use of the center's Internet, computers or network resources. This includes after-hour use and off-site. VTC is not responsible for loss of personal data or information. The center reserves the right to monitor, track, and log network access and use; monitor fileserver space utilization by users; or deny access to prevent unauthorized, inappropriate or illegal activity and may revoke access privileges and/or administer appropriate disciplinary action. The center shall cooperate to the extent legally required with the ISP, local, state and

	federal officials in any investigation concerning or related to the misuse of the center's Internet, computers and network resources. The Joint Operating Committee requires all users to fully comply with this policy and to immediately report any violations or suspicious activities to the Administrative Director or designee.
47 U.S.C. Sec. 254	The Joint Operating Committee establishes the following materials, in addition to those stated in law and defined in this policy, that are inappropriate for access by minors: Defamatory. Lewd, vulgar, or profane. Threatening. Harassing or discriminatory.
Pol. 103, 103.1, 104, 248, 348	Bullying/**Cyberbullying**
Pol. 249	Terroristic.
Pol. 218.2	**Obscene/Pornographic**.
24 P.S. Sec. 4604 20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254	The center reserves the right to restrict access to any Internet sites or functions it deems inappropriate through established Joint Operating Committee policy, or the use of software and/or online server blocking. Specifically, the center operates and enforces a technology protection measure(s) that blocks or filters access to inappropriate matter by minors on its computers used and accessible to adults and students. The technology protection measure shall be enforced during use of computers with Internet access.
24 P.S. Sec. 4604	Upon request by students or staff, the Administrative Director or designee shall expedite a review and may authorize the disabling of Internet blocking/filtering software to enable access to material that is blocked through technology protection measures but is not prohibited by this policy.
24 P.S. Sec. 4610 20 U.S.C. Sec. 6777	Upon request by students or staff, building administrators may authorize the temporary disabling of Internet blocking/filtering software to enable access for bona fide research or for other lawful purposes. Written permission from the parent/guardian is required prior to disabling Internet blocking/filtering software for a student's use. If a request for temporary disabling of Internet blocking/filtering software is denied, the requesting student or staff member may appeal the denial to

	the Administrative Director or designee for expedited review.
4. Delegation of Responsibility	The center shall make every effort to ensure that this resource is used responsibly by students and staff.
24 P.S. Sec. 4604	The center shall inform staff, students, parents/guardians and other users about this policy through employee and student handbooks, posting on the school center web site, and by other appropriate methods. A copy of this policy shall be provided to parents/guardians, upon written request. Users of center networks or center-owned equipment shall, prior to being given access or being issued equipment, sign user agreements acknowledging awareness of the provisions of this policy, and awareness that the center uses monitoring systems to monitor and detect inappropriate use and tracking systems to track and recover lost or stolen equipment. Student user agreements shall also be signed by a parent/guardian. Administrators, teachers and staff have a professional responsibility to work together to help students develop the intellectual skills necessary to discern 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, staff and other authorized individuals have the responsibility to respect and protect the rights of every other user in the center and on the Internet.
24 P.S. Sec. 4601 et seq	**It shall be the responsibility of all members of the center staff to supervise and monitor usage of the online computer network and access to the Internet in accordance with the policy and the Child Internet Protection Act**. Building administrators shall make initial determinations of whether inappropriate use has occurred. **Procedures for disabling or otherwise modifying any technology protection measures shall be the responsibility of the Technology Coordinator or designated representatives.**
20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254 47 CFR Sec. 54.520	The Administrative Director or designee shall be responsible for recommending technology and developing procedures used to determine whether the school's center's computers are being used for purposes prohibited by law or for accessing sexually explicit materials. The procedures 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.
47 U.S.C. Sec. 254	The Administrative Director or designee shall develop and implement administrative regulations that ensure students are educated on network etiquette and other appropriate online behavior, including: 1. Interaction with other individuals on social networking web sites and in chat rooms.
SC 1303.1-A Pol. 249	2. Cyberbullying awareness and response.
5. Guidelines	**The Center strives to provide the most up-to-date technologies and information possible, recognizing their potential to enhance learning. However, network uses involves many ethical questions and issues. Parents/Guardians are urged to discuss center policies and procedures as well as proper and ethical use of networks before approving their use by a child.** **All uses of the center network facilities are intended to support and advance the school center's educational mission or other purposes deemed appropriate by the Joint Operating Committee.** Network accounts shall be used only by the authorized owner of the account for its approved 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. **Computer network accounts assigned to individuals consist of a unique user I.D. code and password combination. Users are not permitted to share accounts or passwords. Temporary guest accounts may be acquired for student or adult visitors by the Technology Coordinator.** **Staff users have access to center-maintained shared drives. Large files should be created on other external media and not stored on the network.** **<u>Incidental Personal Use</u>** **Use of center systems by an individual employee or student for incidental personal use is permitted. Personal use must comply with this policy and all other center policies, procedures and rules, as well as Internet Service Provider**

	(ISP), local, state and federal laws and may not interfere with the employee's job duties and performance, with system operations, with other system users and must not damage the center's systems. Under no circumstances should the employee or student believe that their use is private. **<u>Privacy</u>** **The center reserves the right to monitor, track, log and access any electronic communications, including but not limited to, Internet access and e-mails, at any time for any reason. Users should not have the expectation of privacy in their use of center systems and other center technology, even when used for personal reasons. Further, the center reserves the right, but not the obligation, to access any personal technology device of users brought onto the center's premises or at center events, or connected to the center network, containing center programs or center or students data (including images, files and other information) to ensure compliance with this policy and other center policies, to protect center resources and to comply with the law.** **Everything that users place in their personal files or e-mails should be written as if a third party will review it.** **Users' violations of this policy, any other center policy, or the law may be discovered by routine maintenance and monitoring of the center's computer system, or any method stated in this policy, or pursuant to any legal means.** <u>Safety</u> It is the center's goal to protect users of the network from harassment and unwanted or unsolicited electronic communications. Any network user who receives threatening or unwelcome electronic communications or inadvertently visits or accesses an inappropriate site 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, social networking web sites, etc.
47 U.S.C. Sec. 254 47 CFR Sec. 54.520	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. **Educating all students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.** 3. Safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications.

	4. Prevention of unauthorized online access by minors, including "hacking" and other unlawful activities. 5. Unauthorized disclosure, use, and dissemination of personal information regarding minors. 6. Restriction of minors' access to materials harmful to them. <u>Prohibitions</u> Users 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. Accessing, sending, receiving, transferring, viewing, sharing or downloading obscene, pornographic, lewd, or otherwise illegal materials, images or photographs. 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.
Pol. 814	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. Accessing the Internet, center computers or other network resources without authorization. 19. Disabling or bypassing the Internet blocking/filtering software without authorization. 20. Accessing, sending, receiving, transferring, viewing, sharing or downloading confidential information without authorization. **21. Accessing the Internet, center computers or other network resources without authorization.** **22. Disabling or bypassing the Internet blocking/filtering software without authorization.** **23. Accessing, sending, receiving, transferring, viewing, sharing or downloading confidential information without authorization** <u>Security</u> 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, these 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.

	Individual employees may be exempt from some of these conditions in the course of doing their job duties as assigned by the Administration.
	Software and Copyright
17 U.S.C. Sec. 101 et seq Pol. 814	**Software and noninstructional external data may not be placed on any computer, whether stand-alone or networked to the center's system, without permission from the Director or his/her designee.**
	Users of center resources are reminded that law protects trademarks and/or copyrighted materials. The illegal use of copyrighted materials by students and staff is prohibited. Any data uploaded to or downloaded from the network shall be subject to fair use guidelines, and applicable laws and regulations.
	Center Web Site
	The center shall establish and maintain a web site and shall develop and modify its web pages to present information about the center under the direction of the Administrative Director or designee. All users publishing content on the center web site shall comply with this and other applicable Joint Operating Committee policies.
	Users shall not copy or download information from the center web site and disseminate such information on unauthorized web pages without authorization from the building administrator.
	Electronic Mail
	E-mail has become one of the most used communications tools in both offices and classrooms. The following points are important to keep in mind:
Pol. 801	**1. The software and hardware that provides e-mail capabilities has been publically funded. For that reason, it should not be considered as a private, personal form of communication. The contents of any communication of this type are governed by the Open Records Act. Users must abide and cooperate with any legal request for access to e-mail contents by proper authorities.**
	2. Since e-mail access is provided as a normal operating tool for any employee who requires it to perform his/her job, individual staff e-mail addresses must be shared with interested parents/guardians and community members who request to communicate with staff in this fashion.
	3. Staff should be expected to return e-mail communications to

	parents/guardians or other public members who have a legitimate business request within forty-eight (48) hours of a workday, whenever feasible. Requests from outside agencies for information do not fit into this same category and can be handled with a different timeline or in a manner consistent with previous experience in working with similar requests. Staff should not participate in e-mail surveys without center authorization.
	4. Incoming e-mail that is incorrectly addressed will remain undeliverable. Staff members are not available to personally inspect all messages of this type and forward them to the proper person.
Pol. 216	**5. Requests for personal information on students and staff members should not be honored via e-mail without personal contact and verification of authentication of the person making the request. This relates particularly to any requests for student grades, discipline, attendance or related information. In addition, security information, such as username or password, should not be sent via e-mail for any reason.**
	6. During student contact time in the classroom, e-mail notification should be turned off to prevent interruptions. Staff members should set aside time whenever feasible to check and respond to e-mail messages.
	7. Student names must not appear in the subject area of messages. Initials are acceptable.
	8. Attachments to e-mail messages should include only data files. At no time should program files be attached due to software licensing requirements. In addition, there exists the real possibility that any program files received as attachments over the Internet may include viruses or other very destructive capabilities once they are launched or started. If one receives an attachment like this, the e-mail should be deleted immediately without saving or looking at the attachment. It is your responsibility to notify the Technology Coordinator if you suspect an e-mail has infected your computer.
	9. Subscriptions of Internet listservs should be limited to professional digests due to the amount of e-mail traffic generated by general subscriptions. Subscriptions of Internet listservs are not permitted by students, unless specifically authorized by the administration.
	10. For any student projects that involve e-mail communications, the student shall obtain authorization from the administration to use a center account as a facilitator to the activity, or work with the Technology Coordinator to activate a special project account for a limited time.
	11. Any student or staff member who receives threatening or "hate mail"

	should notify the Technology Coordinator and the administration. An attempt will be made to track down the source of that e-mail and prevent receipt of any additional unsolicited mail. **12. Students shall not access private Internet/e-mail accounts at school.** **13. All e-mail from a school-issued computer may be subpoenaed at any time and used in a court of law as evidence.** **<u>Forgery Prohibited</u>** **Forgery or attempted forgery of electronic messages is prohibited. Attempts to read, delete, copy, or modify the electronic mail of other system users or deliberate interference with the ability of other system users to send/receive electronic mail is prohibited.** <u>Consequences For Inappropriate Use, **Unauthorized and Illegal Use**</u>
24 P.S. Sec. 4604	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 or data belonging to others; copyright violations; and theft of services shall be reported to the appropriate legal authorities for possible prosecution. General rules for behavior and communications apply when using the **center computer systems**, in addition to the stipulations of this policy. Vandalism shall result in loss of access privileges, disciplinary action, and/or legal proceedings. 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.
Pol. 218, 233, 317	Failure to comply with this policy or inappropriate use of the Internet, center network or computers shall result in usage restrictions, loss of access privileges, disciplinary action, and/or legal proceedings. **<u>Liability</u>** **The center does not guarantee service nor is it responsible for damaged or incorrect data. Use of any information obtained on the Internet or other network services must be undertaken at the individual's own risk.** **The center shall not be held liable for the actions of individuals who choose to violate the acceptable uses of the network. In addition, each user and/or user's**

	parent(s)/guardian(s) shall indemnify the center and hold it harmless from and against any damage, liability, loss, or deficiency arising out of or resulting from the user's use and/or misuse of the network. References: School Code – 24 P.S. Sec. 1303.1-A PA Crimes Code – 18 Pa. C.S.A. Sec. 5903, 6312 Child Internet Protection Act – 24 P.S. Sec. 4601 et seq. U.S. Copyright Law – 17 U.S.C. Sec. 101 et seq. Sexual Exploitation and Other Abuse of Children – 18 U.S.C. Sec. 2256 Enhancing Education Through Technology Act – 20 U.S.C. Sec. 6777 Internet Safety, Children's Internet Protection Act – 47 U.S.C. Sec. 254 Children's Internet Protection Act Certifications, Title 47, Code of Federal Regulations – 47 CFR Sec. 54.520 Joint Operating Committee Policy – 103, 103.1, 104, 218, 218.2, 220, 233, 237, 248, 249, 317, 348, **801,** 814