UNITED SCHOOL DISTRICT

SECTION: OPERATIONS

TITLE: ACCEPTABLE USE OF INTERNET, COMPUTERS AND NETWORK RESOURCES

ADOPTED: May 13, 2008

REVISED: February 14, 2012

815. ACCEPTABLE USE OF INTERNET, COMPUTERS AND NETWORK RESOURCES

1. Purpose

The Board supports use of the computers, Internet and other network resources in the district'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 district provides students, staff and other authorized individuals with access to the district's computers, electronic communication systems and network, which includes Internet access, whether wired or wireless, or by any other means.

For instructional purposes, the use of network facilities shall be consistent with the curriculum adopted by the district 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.
3. Authority	The availability of access to electronic information does not imply endorsement by the district of the content, nor does the district guarantee the accuracy of information received. The district 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 district 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 Board declares that computer and network use is a privilege, not a right. The district's computer and network resources are the property of the district. Users shall have no expectation of privacy in anything they create, store, send, delete, receive or display on or over the district's Internet, computers or network resources, including personal files or any use of the district's Internet, computers or network resources. The district reserves the right to monitor, track, and log network access and use; monitor fileserver space utilization by district users; or deny access to prevent unauthorized, inappropriate or illegal activity and may revoke access privileges and/or administer appropriate disciplinary action. The district shall cooperate to the extent legally required with the Internet Service Provider (ISP), local, state and federal officials in any investigation concerning or related to the misuse of the district's Internet, computers and network resources. The Board requires all users to fully comply with this policy and to immediately report any violations or suspicious activities to the Superintendent or designee.
47 U.S.C. Sec. 254	The Board establishes the following materials, in addition to those stated in law and defined in this policy, that are inappropriate for access by minors: 1. Defamatory. 2. Lewd, vulgar, or profane. 3. Threatening.
Pol. 103, 103.1, 104, 248, 348	4. Harassing or discriminatory.
Pol. 249	5. Bullying.

Pol. 218.2	6. Terroristic.
24 P.S. Sec. 4604 20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254	The district reserves the right to restrict access to any Internet sites or functions it deems inappropriate through established Board policy, or the use of software and/or online server blocking. Specifically, the district 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 Superintendent 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 requests 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 Superintendent or designee for expedited review.
4. Delegation of Responsibility	The district shall make every effort to ensure that this resource is used responsibly by students and staff.
24 P.S. Sec. 4604	The district shall inform staff, students, parents/guardians and other users about this policy through employee and student handbooks, posting on the district website, and by other appropriate methods. A copy of this policy shall be provided to parents/guardians, upon written request. Users of district networks or district-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 district uses monitoring systems to monitor and detect inappropriate use. 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 individuals have the responsibility to respect and protect the rights of every other user in the district and on the Internet. Building administrators shall make initial determinations of whether inappropriate use has occurred.
20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254 47 CFR Sec. 54.520	The Superintendent or designee shall be responsible for recommending technology and developing procedures used to determine whether the district'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 Board. 2. Maintaining and securing a usage log. 3. Monitoring online activities of minors.
47 U.S.C. Sec. 254 SC 1303.1-A Pol. 249	The Superintendent 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 websites and in chat rooms. 2. Cyberbullying awareness and response.
5. Guidelines	The United School District 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 school district policies and procedures as well as proper and ethical use of networks before approving their use by a child. All uses of the school district network facilities are intended to support and advance the school district's educational mission or other purposes deemed appropriate by the Board of School Directors.

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 ID 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 members have access to district maintained shared drives. Large files should be created on other external media and not stored on the network.

Incidental Personal Use

Use of district systems by an individual employee or student for incidental personal use is permitted. Personal use must comply with this policy and all other district 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 district's systems. Under no circumstances should the employee or student believe that their use is private.

Privacy

The district 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 district systems and other district technology, even when used for personal reasons. Further, the district reserves the right, but not the obligation, to access any personal technology device of users brought onto the district's premises or at district events, or connected to the district network, containing district programs or district or students data (including images, files and other information) to ensure compliance with this policy and other district policies, to protect district 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.

	Software And Copyright Software and noninstructional external data may not be placed on any computer, whether stand-alone or networked to the district's system, without permission from the Superintendent or his/her designee.
17 U.S.C. Sec. 101 et seq Pol. 814	Users of district resources are reminded that law protects trademarks and/or copyrighted materials. 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. 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: 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 hob, 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 twenty-four (24) hours of a workday, whenever feasible. E-mail does not have to be answered immediately, simply allow enough time so that the twenty-four (24) hour workday turnaround time can be met in most instances. 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 district 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.

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.

9. Subscription 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 building principal.

10. For any student projects that involve e-mail communications, the student shall obtain authorization from the building principal to use a district account as a facilitator to the activity, or work with a network technician to activate a special project account for a limited time.

11. Any student or staff member who receives threatening or “hate mail” should notify a network technician and the building principal. 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 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.

	Prohibitions Students and staff and guests are expected to act in a responsible, ethical and legal manner in accordance with district 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 non-school-related work beyond incidental personal use.
	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, pornography, 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 Board 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 and district systems.

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.

19. Access or transmit gambling, pools for money, including but not limited to, basketball and football, or any other betting or games of chance.

20. Use of proxy sites, V-tunnels and other technologies to circumvent the web filtering system.

Forgery Prohibited

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.

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 district 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.

Consequences For Inappropriate Use

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 of data belonging to others; copyright violations; and theft of services will be reported to the appropriate legal authorities for possible prosecution. 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. **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>Safety</u> 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.
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. 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, sue, and dissemination of personal information regarding minors. 5. Restriction of minors’ access to materials harmful to them. <u>Liability</u> The United School District 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 school district 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 United School District 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

Board Policy – 103, 103.1, 104, 218, 218.2, 220, 233, 237, 248, 249, 317, 348, 814