No.

SECTION: 815

TITLE: ACCEPTABLE USE OF THE ELECTRONIC COMMUNICATIONS SYSTEMS, DEVICES, NETWORK AND INTERNET

ADOPTED: August 2, 2010

REVISED: May 3, 2010

UPPER MERION AREA SCHOOL DISTRICT

	Policy No. 815 **Acceptable Use of the Electronic Communications Systems, Devices, Network and Internet**
	Acceptable Use of the Computers, Network, Internet, Electronic Communications and Information Systems
Purpose	**Upper Merion Area School District ("School District") provides employees, students and guests ("Users") with access to the School District's electronic communications systems and network. This access includes internal Upper Merion Area hosted applications as well as Internet access, whether wired or wireless, or by any other means.** Computers, electronic devices, network, Internet, electronic communications and information systems (collectively "CIS systems") provide vast, diverse and unique resources. The Board will provide access to the School District's CIS systems for Users in order to access information, research, and collaboration to facilitate learning and teaching to foster the educational purpose and mission of the School District. **Usage** The School District's CIS systems must be used primarily for education-related purposes and performance of School District job duties. Incidental personal use of School District electronic devices is permitted for Users so long as such use does not interfere with educational practices, system operations, or with other system users. Personal use must comply with this policy and all other applicable School District policies, procedures and rules contained in this policy, as well as Internet service provider ("ISP") rules and regulations, and all applicable local, state and federal laws. Personal use must not damage and/or otherwise impair the School District's CIS systems. Users may also be permitted to use Users' personal electronic devices while on School District property, at School District events and/or in connection with the School District's CIS systems, but only in strict compliance with this policy and all other applicable School District policies, procedures and rules, as well as ISP rules and regulations and all applicable local, state and federal laws. Use of personal electronic devices must not interfere with educational practices, system operations, or other system users, and/or otherwise damage or impair the School District's CIS systems.

Security

The School District intends to strictly protect its CIS systems against numerous outside and internal risks and vulnerabilities. Users are important and critical players in protecting these School District assets and in lessening the risks that can harm 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 Technology Director. Conduct otherwise will result in actions further described in Section 12 (Consequences for Inappropriate, Unauthorized and Illegal Use) of this Policy and as provided in other relevant School District policies.

Definitions

1. Access to the Internet – A device shall be considered to have access to the Internet if the device is connected to a network that has access to the Internet, whether by wire, wireless, cable, or any other means.

2. Child Pornography - Under federal law, 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:

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

   c. Such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

   Under Pennsylvania law, 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.

3. Electronic Device – Any School District owned, leased or licensed or User owned: personal hardware, software, or other technology used on School District premises or at School District events, connected to the School District CIS systems, and/or containing School District programs or data. Electronic devices include, but are not limited to, laptop computers, cell phones, wireless devices and similar technologies.

4. Electronic Communications Systems – Any messaging, collaboration, publishing, broadcast, or distribution system that depends on electronic communications resources to create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, or print electronic records for purposes of communication across electronic communications network systems between or among individuals or groups, that is either explicitly denoted as a system for

electronic communications or is implicitly used for such purposes.

5. Educational Purpose - Includes use of the CIS systems for classroom activities, professional or career development, and to support the School District's curriculum, policy and mission statement.

6. Harmful to Minors – Under federal law, any picture, image, graphic image file or other visual depictions that:

   a. taken as a whole, with respect to minors, appeals to the prurient interest in nudity, sex, or excretion;

   b. 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 content, actual or simulated normal or perverted sexual acts, or lewd exhibition of the genitals, and

   c. taken as a whole lacks serious literary, artistic, political, or scientific value as to minors.

   Under Pennsylvania law, any depiction or representation in whatever form, of nudity, sexual conduct, sexual excitement, or sadomasochistic abuse, when it:

   a. predominantly appeals to the prurient, shameful, or morbid interest of minors;
   b. is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable material for minors; and
   c. taken as a whole, lacks serious literary artistic, political, educational or scientific value for minors.

   For purposes of this policy, any text or audio depictions of such matters shall be included in this definition.

7. Inappropriate Matter – Inappropriate matter includes, but is not limited to, visual, graphic, text and other form of obscene, sexually explicit, child pornographic, or other material that is harmful to minors, hateful, illegal, defamatory, lewd, vulgar, profane, rude, inflammatory, threatening, harassing, discriminatory (as it pertains to race, color, religion, national origin, gender, material status, age, sexual orientation, political beliefs, receipt of financial aid, or disability), violent, bullying, terroristic, and/or advocates the destruction of property.

8. Incidental Personal Use – Use of School District CIS systems by an individual User for occasional personal communications.

9. Minor – For purposes of compliance with the Children's Internet Protection Act ("CIPA"), an individual who has not yet attained the age of seventeen. For other purposes, minor shall

mean any person under the age of eighteen (18).

10. Network – A system that links two or more electronic devices, including all components necessary to effect the operation.

11. Obscene – Under federal and Pennsylvania law, any material if:

    a. the average person, applying contemporary community standards, would find that the material, taken as a whole, appeals to the prurient interest;
    b. the subject matter depicts or describes in a patently offensive way, sexual conduct described in the law to be obscene; and
    c. the subject matter, taken as a whole, lacks serious artistic, political, educational or scientific value.

12. School District Premises –School District Premises shall include all buildings, facilities, parking areas and other grounds, owned or leased by the School District and/or otherwise under the control of the School District, as well as all school buses, school vehicles and other conveyances used to transport School District students. As it relates to School District students attending the Central Montco Technical High School ("CMTHS"), School District Premises shall also include all buildings, facilities, parking areas and other grounds owned or leased by the CMTHS and/or otherwise under the control of CMTHS.

13. Sexual Act and Sexual Contact – As defined at 18 U.S.C. § 2246(2), 18 U.S.C. § 2246(3), and 18 Pa.C.S.A. § 5903.

14. Technology Protection Measure(s) (TPM) – A specific technology that is intended to block or filter access to content that is obscene, child pornography or harmful to minors.

Authority

1. Access to the School District's CIS systems through school resources is a privilege, not a right. These, as well as the user accounts and information, are the property of the School District, which reserves the right to deny access to prevent further unauthorized, inappropriate or illegal activity, and may revoke those privileges and/or administer appropriate disciplinary action. The School District will cooperate fully with ISP, local, state and federal officials in any investigation concerning or related to the misuse of the CIS systems.

2. It is often necessary to access user accounts in order to perform routine maintenance and security tasks. System administrators have the right to access User accounts by interception, and by retrieval of stored communication, to maintain the system. Users have no privacy expectation in the contents of their personal files or any of their use of the School District's CIS systems. The School District reserves the right to monitor, track, log and access CIS systems use and to monitor and allocate resources.

3. The School District reserves the right to restrict access to any Internet sites or functions it may deem inappropriate through software blocking or general policy. Specifically, the School District operates and enforces technology protection measure(s) that block or filter online activities of Users on its electronic devices so as to filter or block inappropriate matter. Measures designed to restrict access to material harmful to students may be disabled to enable an staff to access *bona fide* research or for another lawful purpose.

4. The School District reserves the right, but not the duty, to monitor, track, log, access and report all use of the School District's CIS systems and School District electronic devices, as well as use by School District employees and students, of any personal electronic devices on School District premises or at School District events, connected to the School District network, and/or containing School District programs or data (including images, files, and other information), to the fullest extent permitted by law, to insure compliance with this policy and other School District policies, to protect the School District's resources, and to comply with the law. The School District further reserves the right, but not the duty, to monitor, track, log, access and report all use by Guest of personal electronic devices connected to the District network and/or containing School District programs or data, pursuant to the law, to insure compliance with this policy, and other School District policies, to protect the School District's resources, and to comply with the law.

5. The School District reserves the right to restrict or limit usage of lower priority CIS systems and computer uses when network and computing requirements exceed available capacity according to the following priorities:

   a. Highest – uses that directly supports the education of the students.

   b. Medium – uses that indirectly benefit the education of the student.

   c. Lowest – uses that include reasonable and limited educationally-related interpersonal communications and incidental personnel communications.

   d. Forbidden – all activities in violation of this policy.

6. The School District additionally reserves the right to:

   a. Determine which CIS systems services will be provided through School District resources.

   b. View and monitor network traffic, file server space, processor, and system utilization, and all applications provided through the network and communications systems, including e-mail.

   c. Remove excess e-mail or files taking up excessive server resources as determined by the

	Technology Director. Notice will be provided to remove excess e-mail or files before being purged. d. Revoke user privileges, remove user accounts, or refer to legal authorities when violation of this and any other applicable School District policies occur or state or federal law is violated, including, but not limited to, those governing network use, copyright, security, privacy, employment, and destruction of School District resources and equipment.
Responsibility	1. Due to the nature of the Internet as a global network connecting electronic devices around the world, inappropriate matter, can be accessed through the network and electronic communications systems. Because of the nature of the technology that allows the Internet to operate, the School District cannot completely block access to these resources. Accessing these and similar types of resources may be considered an unacceptable use of school resources and will result in actions explained further in Section 12 Consequences for Inappropriate, Unauthorized and Illegal Use, found on page 16 of this policy and as provided in relevant School District policies. 2. Users must become proficient in the use of the School District's CIS systems and software relevant to the use of the School District's CIS systems**;** practice proper netiquette and School District ethics; and agree to the requirements of this policy.
Delegation of Responsibility	1. The Technology Director and/or designee will serve as the coordinator to oversee the School District's CIS systems and will work with other regional or state organizations as necessary, to educate users, approve activities, provide leadership for proper training in the use of the CIS systems and the requirements of this policy, establish a system to insure adequate supervision of the CIS systems, maintain executed user agreements, and interpret and enforce this policy. 2. The Technology Director and/or designee will establish a process for: setting up individual user, class and service accounts; setting quotas for resource allocation; establishing a retention schedule; and establishing the School District electronic device security/threat protection mechanisms. 3. Unless otherwise denied for cause, student access to the CIS systems resources shall be through supervision by the professional staff. Administrators, teachers and staff have the responsibility to work together to help students develop the skills and judgment required to make effective and appropriate use of the resources. All users have the responsibility to respect the rights of all other users within the School District and School District CIS systems, and to abide by the rules established by the School District, its ISP, local, state and federal laws.
Guidelines	1. Access to the CIS Systems

a. CIS systems user accounts will be used only by authorized owners of the accounts for authorized purposes.

b. An account will be made available according to a procedure developed by appropriate School District authorities.

c. CIS System. The School District's Acceptable Use of the Computers, Network, Internet, Electronic Communications, and Information Systems Policy, as well as other relevant School District policies, will govern use of the School District's CIS systems for Users. **U**se of the CIS systems will also be governed by the other relevant School District policies.

d. Guest Access. Guests may receive individual access to CIS Systems with the approval of the Technology Director and/or designee. Guests are considered Users and must adhere to all applicable district policies.

e. Access to all data on, taken from, or compiled using School District electronic devices is subject to inspection and discipline. Users have no right to expect that School District information placed on Users' personal electronic devices, external media, networks, and Internet is beyond the access of the School District. The School District reserves the right to access Users' personal equipment for School District information.

2. Parental Notification and Responsibility

The School District will notify parents/guardians about the policies governing the use of School District CIS systems and the use of electronic devices on School District premises. This policy contains restrictions on accessing inappropriate material. There is a wide range of material available on the Internet, some of which may not be fitting with the particular values of the families of the students. It is not practically possible for the School District to monitor and enforce a wide range of social values in student use of the Internet. Further, the School District recognizes that parents bear primary responsibility for transmitting their particular set of family values to their children. The School District will encourage parents/guardians to specify to their child(ren) what material is and is not acceptable for their child(ren) to access through the School's District's CIS system. Parents/guardians are responsible for monitoring their children's use of the School District's CIS systems when they are accessing the systems outside of School District premises.

3. School District Limitation of Liability

The School District makes no warranties of any kind, either expressed or implied, that the functions or the services provided by or through the School District's CIS systems will be error-free or without defect. The School District does not warrant the effectiveness of Internet filtering. The electronic information available to users does not imply endorsement of the content by the

School District, nor is the School District responsible for the accuracy or quality of the information obtained through or stored on the CIS systems. The School District shall not be responsible for any damage users may suffer, including but not limited to, information or equipment that may be lost, damaged, delayed, mis-delivered, or unavailable when using electronic devices**.** The School District shall not be responsible for material that is retrieved through the Internet, or the consequences that may result from them. The School District shall not be responsible for any unauthorized financial obligations, charges or fees resulting from or through access to the School District's CIS systems. In no event shall the School District be liable to the User for any damages whether direct, indirect, special or consequential, arising out the use of the CIS systems or electronic devices. To the contrary, should a User incur charges, such charges will be the User's responsibility.

4. Prohibitions

Users are prohibited from using the School District's CIS systems for illegal, inappropriate, unacceptable, or unethical purposes. Such activities engaged in by Users are strictly prohibited and illustrated below. The School District reserves the right to determine if any activity not appearing in the list below constitutes an acceptable or unacceptable use of the CIS systems.

Students who bring personal electronic devices to school shall use these devices in compliance with the guidelines set forth by School District Administration. Further, such students shall not be permitted to connect such devices to the School District's CIS or through the School District's CIS to outside networks or resources.

a. General Prohibitions – Users are prohibited from using School District CIS systems to:

(1) Communicate about non-work or non-school related communications unless the use comports with this policy's definition of incidental personal use.

(2) Access or transmit material that is harmful to minors and/or users, indecent, obscene, pornographic, child pornographic, terroristic, or advocates the destruction of property.

(3) Access or transmit material likely to be offensive or objectionable to recipients including, but not limited to, that which may be defamatory, inaccurate, obscene, sexually explicit, lewd, hateful, harassing, discriminatory (as it pertains to race, color, religion, national origin, gender, marital status, age, sexual orientation, political beliefs, receipt of financial aid, or disability), violent, vulgar, rude, inflammatory, threatening, profane, pornographic, offensive, terroristic and/or illegal.

(4) Cyberbullying.

(5) Access or transmit gambling, pools for money, or any other betting or games of

chance.

(6) Participate in discussion or news groups that cover inappropriate and/or objectionable topics or materials, including those that conform to the definition of inappropriate matter in this policy.

(7) Send terroristic threats, hateful mail, harassing communications, discriminatory remarks, and offensive or inflammatory communications.

(8) Participate in unauthorized communications that are not for school-related purposes or required for employees to perform their job duties, except for incidental personal use as allowed under this Policy.

(9) Facilitate any illegal activity.

(10) Engage in commercial, for-profit, or any business purposes (except where such activities are otherwise permitted or authorized under applicable School District policies); conduct unauthorized fund raising or advertising on behalf of the School District and non-school School District organizations; resell of School District computer resources to individuals or organizations; or use the School District's name in any unauthorized manner that would reflect negatively on the School District, its employees, or students.

(11) Political lobbying.

(12) Install, distribute, reproduce or use copyrighted software on School District computers or copy School District software to unauthorized computer systems, intentionally infringing upon the intellectual property rights of others or violating a copyright. See Section 8 Copyright Infringement on page 14 of this Policy and the School District's Copyright Policy for additional information.

(13) Install computer hardware, peripheral devices, network hardware or system hardware. The authority to install hardware or devices on School District computers is restricted to the Technology Director or designee.

(14) Encrypt messages or data using encryption software that is not authorized by the School District from any access point on School District equipment or School District property. Users must use School District approved encryption to protect the confidentiality of sensitive or critical information in the School District's approved manner.

(15) Violate the privacy**,** confidentiality or security of electronic information.

(16) Use the systems to send any School District information to another party, except in

the ordinary course of business as necessary or appropriate for the advancement of the School District's business, or educational interest.

(17) Send unsolicited commercial electronic mail messages, also known as spam.

(18) Create personal web pages utilizing School District resources without administrative approval.

b. Access and Security Prohibitions

Users must immediately notify the Technology Director and/or designee if they have identified a possible security problem. Users must read, understand and comply with this policy that includes network, Internet usage, electronic communications, telecommunications, non-disclosure and physical information security policies. The following activities related to access to the School District's CIS systems, and information are prohibited:

(1) Misrepresentation (including forgery) of the identity of a sender or source of communication.

(2) Acquiring or attempting to acquire passwords of others or giving your password to another. Users will be held responsible for the result of any misuse of their accounts.

(3) Using or attempting to use computer accounts of others. This includes instances where the Users' account was left unattended and accessible to others, whether intentionally or through negligence.

(4) Altering a communication originally received from another person or computer with the intent to deceive.

(5) Using School District resources to engage in any illegal act, which may threaten the health, safety or welfare of any person or persons.

(6) Disabling or circumventing any School District security; software or hardware.

(7) Transmitting electronic communications anonymously or under an alias unless authorized by the School District.

c. Operational Prohibitions

The following operational activities and behaviors are prohibited:

(1) Interference with or disruption of the CIS systems, network accounts, services or

equipment or personal electronic devices of others.

(2) Altering or attempting to alter files, system security software/hardware or any CIS systems without authorization.

(3) Unauthorized scanning of the CIS systems for security vulnerabilities.

(4) Attempting to alter any School District computing or networking components without authorization or beyond one's level of authorization.

(5) Attempting to create unauthorized network connections or any unauthorized extension or re-transmission of any computer, electronic communications systems, or network services, whether wired, wireless, cable, or by other means.

(6) Connecting unauthorized hardware and electronic devices to the CIS systems.

(7) Loading, downloading, or use of unauthorized games, music, video**,** programs, files, or other electronic media.

(8) Intentionally damaging or destroying the integrity of the School District's electronic information, computer hardware, software or any CIS systems.

(9) Failing to comply with requests from the Technology Director or designee to discontinue activities that threaten the operation or integrity of the CIS systems.

5. Content Guidelines

Information electronically published on the School District's CIS systems shall be subject to the following guidelines:

a. Published documents including but not limited to audio, image and video clips or conferences, may not include student information in compliance with School District Policy and administrative guidelines related to web standards.

b. Documents, web pages, electronic communications, or video conferences may not contain objectionable materials or point directly or indirectly to objectionable materials.

c. Documents, web pages and electronic communications, must conform to all School District policies and guidelines, including the copyright policy.

6. Due Process

a. The School District will cooperate with the School District's ISP, local, state, and federal officials to the extent legally required in investigations concerning or relating to any illegal activities conducted through the School District's CIS systems.

b. If users are entitled to due process rights for discipline resulting from the violation of this policy, they will be provided such rights.

c. The School District may terminate the account privileges with or without providing notice to the user.

7. User's Consent to District Access and Disclosure

a. Users' violations of this Policy, any other School District policy, or the law may be discovered by routine maintenance and monitoring of the School District system, or any method stated in this policy, or pursuant to any legal means. User consents to the School District's disclosure of information related to such violations as determined necessary by the School District to protect the School District's resources and to comply with the law.

b. The School District shall have the right, but not the obligation, to monitor, track, log and access any electronic information or communications relating to use of the School District CIS systems and electronic devices. Users should not have the expectation of privacy in their use of the School District's CIS systems, and other School District technology, even when used for personal reasons. Further, the School District shall have the right, but not the obligation, to access any personal electronic device of students and employees brought onto the School District's premises or at School District events, and/or any personal electronic device of any User connected to the School District network or containing School District programs or data, to insure compliance with this policy and other School District policies, to protect the School District's resources, and to comply with the law.

c. Users' execution of the User Acknowledgment shall constitute consent to the exercise of the aforesaid rights by the School District, as well as the confiscation of any personal electronic device and/or the disclosure of any information obtained by the School District pursuant to the exercise of the aforesaid rights, as determined necessary by the District to insure compliance with this policy and other School District policies, to protect the School District's resources and to comply with the law. As it relates to personal electronic devices, such devices may be searched once confiscated where there is reasonable suspicion that they contain information relating to a violation of a School District policy or code of conduct.

8. Copyright Infringement and Plagiarism

   a. Federal laws, cases, and guidelines pertaining to copyright will govern the use of material accessed through the School District resources. Users will make a standard practice of requesting permission from the holder of the work and complying with license agreements. Employees will instruct students to respect copyrights, request permission when appropriate, and comply with license agreements and employees will respect and comply as well.

   b. Violations of copyright law can be a felony and the law allows a court to hold individuals personally responsible for infringing the law. The School District does not permit illegal acts pertaining to the copyright law. Therefore, any user violating the copyright law does so at their own risk and assumes all liability.

   c. The illegal installation of copyrighted software or files for use on the School District's computers is expressly prohibited. The license of any copyrighted software or files must be owned by the School District.

   d. School District guidelines on plagiarism will govern use of material accessed through the School District's CIS systems.

9. Selection of Material

   a. Board policies on the selection of materials will govern use of the School District's CIS systems.

   b. When using the Internet for class activities, teachers will select material that is appropriate in light of the age of the students and that is relevant to the course objectives. Teachers will preview the materials and web sites they require or recommend students access to determine the appropriateness of the material contained on or accessed through the web site. Teachers will provide guidelines and lists of resources to assist their students in channeling their research activities effectively and properly. Teachers will assist their students in developing the critical thinking skills necessary to ascertain the truthfulness of information, distinguish fact from opinion, and engage in discussions about controversial issues while demonstrating tolerance and respect for those who hold divergent views.

10. School District Web Site

   a. The School District will establish and maintain a Web Site and will develop and modify its Web pages that will present information about the School District under the direction of the Technology Director or designee. The Technology Director, building administrators or their designees will be responsible for the approval of information posted on the website.

All web pages will be posted at the discretion of and by the Technology Director, building administrators or their designees, unless otherwise determined appropriate by the Technology Director.

b. School District employees may not officially or unofficially represent the school district on non-district websites. The Upper Merion Area School District is not liable for information posted on non-district sites.

c. Groups associated with the School District as School District curricular, co-curricular, or auxiliary groups, including but not limited to PTA's, booster clubs, band associations or other associations representing official school district activities, may only establish or maintain websites representing such School District-affiliated groups upon agreement to comply with guidelines created by the School District Administration. Such guidelines will include general content guidelines and a requirement to provide the Technology Director with a valid password permitting administrative access to the site.

d. The District shall not place links on its own web site, except to the above affiliated groups which are under the direction of the District, and except as specified below.

e. Classes and teachers may establish web pages that comply with this policy and any administratively created guidelines to present information about the class activities or for other curricular purposes. Teachers are responsible for any content created by their students posted on such sites. Anyone creating such a web page or site outside the direct control of the School District must notify the Technology Director and provide him or her with UserID's and passwords with sufficient access to permit administration of the site when necessary.

f. Any links occurring on School District web pages must accord with the law and must only link to sites that have an educational purpose. Links may not be identified with defamatory, slanderous, libelous or inappropriate language. No attempt should be made to misrepresent the location of a link.

g. Only users authorized to do so by the Technology Director may post information on the authorized School District websites. All websites operated under authority of this policy, and the content therein, are subject to prior approval of and periodic review by the Technology Director.

h. The Technology Director reserves the right to remove any material posted to any of the websites authorized pursuant to this policy.

11. <u>Safety & Privacy</u>

a. To the extent legally required, users of the School District's CIS systems will be protected from harassment or commercially unsolicited electronic communication. Any user who receives threatening or unwelcome communications must immediately take them to the Technology Director and/or designee.

b. A user may not disclose, use or disseminate confidential, electronic or personal information about themselves or other users without appropriate consent, use for educational purpose and in compliance with School District Policy _____.

c. Student users will agree not to physically meet with someone they have only met online unless they have parent consent.

12. Consequences for Inappropriate, Unauthorized and Illegal Use

a. General rules for behavior, ethics, and communications apply when using the CIS systems and information, in addition to the stipulations of this policy. Users must be aware that violations of this policy or other policies, or for unlawful use of the CIS systems may result in loss of CIS access and a variety of other disciplinary actions and/or legal proceedings on a case-by-case basis. This policy incorporates all other relevant School District policies.

b. The user is responsible for damages to the network, equipment, electronic communications systems, and software, including incidental or unintended damage, resulting from willful or deliberate violations of this policy.

c. Violations as described in this policy may be reported to the School District, appropriate legal authorities, whether the ISP, local, state, or federal law enforcement. The School District will cooperate to the extent legally required with authorities in all such investigations.

d. Vandalism may result in cancellation of access to the School District's CIS systems and resources and is subject to discipline.

13. Internet Safety Programs.

The District Administration shall assure that the on-line activities of Students are monitored and that Students are provided educational programs regarding appropriate on-line behavior, including interacting with other individuals on social networking websites and in chat rooms and cyber bullying awareness and response. Plans for educating students as set forth above shall be periodically reviewed and updated by the District Administration.

	Policy No. 815 **Acceptable Use of the Electronic Communications Systems, Devices, Network and Internet**
	14. User Acknowledgement The Board requires that each User sign a document indicating their understanding of, and agreement and intent to adhere to the terms of this policy.
	References: Pennsylvania Children's Internet Protection Act, 24 P.S. Section 4601 et seq. Pennsylvania Crimes Code, 18 Pa.C.S.A. Sections 5933 and 6312 Pennsylvania Public School Code, 24 P.S. Sections 5-510, 13-1317.1, and 13-1303.1A Pennsylvania Wiretapping and Electronic Surveillance Act, 18 P.A.C.A. Section 5701 et seq. Federal Children's Internet Protection Act, 20 U.S.C.S. Sections 6301 note and 6777 Federal Communication Act, 47 U.S.C.S. Section 254 Federal Computer Fraud and Abuse Act, 18 U.S.C.S. Section 1030 Federal Crimes and Procedures, 18 U.S.C.S. Section 1460 Federal Electronic Communications Privacy Act, 18 U.S.C.S. Sections 2511 and 2520 Federal Protecting Children in the 21st Century Act, Pub.L. No. 110-385, Title II, 122 Stat. 4096 (2008) Federal Stored Communications Act, 18 U.S.C. Section 2701