EASTON AREA SCHOOL DISTRICT

SECTION: OPERATIONS

TITLE: ACCEPTABLE USE OF TECHNOLOGY AND THE INTERNET

ADOPTED: July 20, 2006

REVISED: June 28, 2012

815. ACCEPTABLE USE OF TECHNOLOGY AND THE INTERNET

1. Purpose

The Easton Area School District provides employees, students, and guests with access to the district's network and to the Internet, whether wired or wireless, in order to facilitate learning, teaching and daily operations through interpersonal communications and access to information, research and collaboration.

Access to the district's network shall be for specific education-related purposes to access information and research; to collaborate; to facilitate learning and teaching; and to foster the educational mission, vision and beliefs of the district.

The purpose of this policy is to help students, employees and guests understand acceptable use of the district's computer network, including, but not limited to, district-issued laptop computers and all devices logged into the district's computer network, used during and after regular work hours.

Any district-owned technology used during the school/work day or used off district property shall be considered part of the district's computer network. Guidelines for acceptable use during work hours extend to use of district technology after work hours.

Acceptable use of the district network and associated technology is rooted in current district policy, accepted rules of network etiquette, federal and state laws, the Code of Professional Practice and Ethics, and the Public School Code.

2. Authority

The electronic information available to students and staff 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 operates and enforces technology protection measures that filter online activities of all users so as to filter or lock inappropriate matter on the Internet.

The district shall not be responsible for any unauthorized charges or fees resulting from access to the Internet.

	All communications on the district's network are property of the Easton Area School District. Users have no privacy expectations in the contents of their personal files or any of their use of the district's network. The district reserves the right to monitor, track and/or log user access, monitor and allocate fileserver space, and access and archive all user files.
	The level of access that employees have to school computers, network, and Internet services shall be based upon specific employee job requirements and needs.
	For Users, the district's network must be used for education-related purposes and performance of district job duties. The policy does recognize that employees may use district technologies for "incidental" personal use, but there should be no expectation of privacy. The policy defines **incidental use** as casual, insignificant or occasional "that does not impact an employee's duties or impede educational operations.
Pol. 218, 233, 317, 417, 517	The Easton Area School District establishes that network use is a privilege, not a right. Inappropriate, unauthorized and illegal use will result in cancellation of those privileges and appropriate disciplinary action. The district will cooperate to the extent legally required with Internet Service Provider (ISP), local, state and federal officials in any investigation concerning or related to the misuse of the district's network.
3. Definitions 18 U.S.C. Sec. 2256	**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.
	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	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.

	Computer - includes any district-owned, leased or licensed hardware, software, or other technology used on district premises or at district events, or connected to the district network. Computer includes, but is not limited to: desktop and laptop computers, mobile devices (cell phones, mp3 players, tablets, pagers, etc.), printers, cables, and other peripherals including thumb and flash drives, specialized electronic equipment used for students' special educational purposes, and any other such technology developed.
20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254	**Harmful to Minors** - under federal law, any picture, image, graphic image file or other visual depictions that: 1. Is taken as a whole, with respect to minors, appeals to the 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 content, actual or simulated normal or perverted sexual acts, or lewd exhibition of the genitals. 3. Taken as a whole lacks serious literary, artistic, political, educational or scientific value as to minors.
18 Pa. C.S.A. Sec. 5903	Under Pennsylvania law, 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. 3. Taken as a whole, lacks serious literary, artistic, political, educational or scientific value for minors.
	Minor - for purposes of compliance with the Children's Internet Protection Act ("CIPA"), an individual who has not yet attained the age of seventeen (17). For other purposes, minor shall mean the age of minority as defined in the relevant law.
	Network - a system that links two (2) or more computer systems, including all components necessary to effect the operation, including, but not limited to: computers, copper and fiber cabling, wireless communications and links, equipment closets and enclosures, network electronics, telephone lines, printers and other

	peripherals including thumb and flash drives, storage media, software, and other computers and/or networks to which the network may be connected, such as the Internet or those of other institutions.
	Obscene - under federal law, analysis of the material meets the following elements:
	1. Whether the average person, applying contemporary community standards, would find that the material, taken as a whole, appeals to the prurient interest.
	2. Whether the work depicts or describes, in a patently offensive way, sexual conduct specifically designed by the applicable state or federal law to be obscene.
	3. Whether the work taken as a whole lacks serious literary, artistic, political, educational, or scientific value.
18 Pa. C.S.A. Sec. 5903	Under Pennsylvania law, analysis of the material meets the following elements:
	1. The average person, applying contemporary community standards, would find that the material, 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.
	3. The subject matter, taken as a whole lacks serious literary, artistic, political, educational or scientific value.
	Sexual Act and Sexual Contact - as defined at 18 U.S.C. Sec. 2246, and at 18 Pa. C.S.A. Sec. 5903.
	Social Networking Sites - are web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system. It also includes other types of websites that allow users to share content, interact with each other and develop communities around similar interests. This definition shall expressly include community-based websites, online discussion forums, chat rooms and other social spaces online. For the purposes of this policy, **Social Networking Sites** shall also include blogs. **Blog** is a website that contains an online personal journal with reflections, comments, and often hyperlinks provided by the writer.

47 U.S.C. Sec. 254	**Technology Protection Measure(s) -** a specific technology that blocks or filters Internet access to visual depictions that are obscene, child pornography or harmful to minors. **Visual Depictions -** undeveloped film and videotape and data stored on computer disk or by electronic means which is capable of conversion into a visual image but does not include mere words.
4. Delegation of Responsibility	The district shall make every effort to ensure that students and staff use network resources responsibly. These resources may include, but are not limited to, network user accounts, computers, the Internet, email, blogs and other second and third generation web services. The Superintendent or designee will serve as the coordinator to oversee the district's network and will work with others to educate users, approve activities, maintain executed user agreements and interpret and enforce this policy. In coordination with Technology Support, the Director of Instructional Technology and District Services will establish a process for establishing user accounts, establishing quotas for fileserver storage space, establishing a document and email retention procedure, as well as establishing a virus protection process.
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 may deem inappropriate through general policy, software blocking or online server blocking. Specifically, the district operates and enforces technology protection measure(s) that block or filter online activities of minors on its computers used and accessible to adults and students so as to filter or block inappropriate matter on the Internet. Inappropriate matter includes, but is not limited to visual, graphic, text and any other form of obscene, sexually explicit, child pornographic, or other material that is harmful to minors, or that is hateful, illegal, defamatory, lewd, vulgar, profane, rude, inflammatory, threatening, 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, bullying, terroristic, and advocates the destruction of property. Measures designed to restrict adults' and minors' access to material harmful to minors may be disabled to enable an adult or student to access bona fide research, not within the prohibitions of this policy, or for another lawful purpose. No person may have access to material that is illegal under federal or state law. Expedited review and resolution of a claim that the policy is denying a student or adult to access material will be enforced by an administrator, supervisor, or their designee upon the receipt of a written consent from a parent/guardian for a student, and upon the written request from an employee.

SC 1303.1-A 47 U.S.C. Sec. 254 Pol. 252	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 network resources. This includes educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response. All users have the responsibility to respect the rights of all other users within the district and to abide by the rules established by the district, local, state and federal laws. The district will notify staff and parents/guardians annually about the network systems and the policies governing their use. A copy of this policy shall be posted on the district's website and available directly from the Office of the Superintendent.
	While the district understands the value of current social networking sites, it prohibits employees from developing virtual relationships with students beyond the educational program through social networking tools. Faculty members must acquire permission from the building administrator prior to engaging in social networking within the educational program. If such a project is approved, the faculty member overseeing the project must communicate the project information to the parents of all students involved in the project, informing the parent of the nature of the assignment and their right to choose an alternate assignment.
	<u>Cyberbullying</u>
Pol. 218, 248, 252	Cyberbullying and online harassment is unacceptable behavior. Cyberbullying and online harassment occurring on the district's network, during the school day, on school grounds and/or at school events will not be tolerated. Cyberbullying and online harassment can occur through email, texting, social media, etc. It can occur in the form of direct harassment/bullying; threatening communications; falsely impersonating another individual online with the intent to harass, embarrass, or otherwise psychologically harm another individual; etc.
	Engaging in these behaviors, or any online activities intended to harm (physically or emotionally) another person, on the district's network could result in severe disciplinary action and loss of privileges. In some cases, cyberbullying can be a crime. Students should remember that their online activities on the district's network and/or on district technology may be monitored and retained.
	<u>Student Training</u>
SC 1303.1-A 47 U.S.C. Sec. 154 Pol. 252	The district shall provide, at least once per school year, training to students regarding safety and the Internet. This training shall include information about this policy as well as additional information regarding appropriate online behavior, including

proper interactions with other individuals on social networking sites and in chat rooms. The training shall also include information regarding cyberbullying and appropriate responses to cyberbullying.

Parental Notification And Responsibility

The district will notify the parents/guardians about the district's computer network systems and the policies governing their use. 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 district to monitor and enforce a wide range of social values in student use of the Internet. Further, the district recognizes that parents/guardians bear primary responsibility for transmitting their particular set of family values to their children. The district will encourage parents/guardians to specify to their children what material is and is not acceptable for their children to access through the district's computer network systems.

Student Privacy Rights And Employee Sites

All teachers and district employees must be aware that all personal and professional blogs and social networking communications, even when authored/utilized outside of the school day and off school grounds, are subject to FERPA and other student privacy laws, including those found in the IDEA. Dissemination of private student information over these sites is expressly prohibited by law and this policy.

School District Limitation Of Liability

The district makes no warranties of any kind, either expressed or implied, that the functions or the services provided by or through the district's computer network systems will be error-free or without defect. The district does not warrant the effectiveness of Internet filtering. The electronic information available to users does not imply endorsement of the content by the district. The district is neither responsible for nor guarantees the accuracy or quality of the information obtained through or stored on the district's computer network systems. The district shall not be responsible for any damage users may suffer, including but not limited to, information that may be lost, damaged, delayed, mis-delivered, or unavailable when using the network and electronic communications systems. The district shall not be responsible for material that is retrieved through the Internet, or the consequences that may result from them. The district shall not be responsible for any unauthorized financial obligations, charges or fees resulting from access to the district's computer network systems. In no event shall the district be liable to the user for any damages whether direct, indirect, special or consequential, arising out of the use of the district's computer network systems.

	Easton Area School District provides the guidelines as per Section 5. The building administrator shall have the authority to determine what is inappropriate use based on district guidelines. The building administrator shall notify the Director of Instructional Technology and District Services when issues outside the guidelines are encountered.
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 implementing technology and procedures to determine whether the district's computers are being used for purposes prohibited by law or for accessing sexually explicit materials in violation of this policy. Because of the nature of the technology that allows the Internet to operate, the school district cannot completely block access to these explicit materials. Accessing these and similar types of resources may be considered an unacceptable use of school resources and may result in disciplinary actions and/or denial of Internet privileges. 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. 2. Maintaining and securing a usage log. 3. Monitoring online activities of minors.
	<u>Use Of Non-District Internet Access During School Hours, On School Grounds Or At School Functions</u> The provisions of this policy shall also apply to student and employee use of the Internet and other network access not provided by the district, including personal Internet access through laptops and mobile devices, when such access occurs during school hours, on school grounds, or at school functions.
5. Guidelines	Network accounts shall be used only by the authorized owner of the account for its approved purpose. Network users shall respect the privacy of other users on the system.

	Prohibitions Students and employees 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, the Code of Professional Practice and Ethics, and the Public School Code. Additionally, this expectation applies to all users of district-owned technology. Specifically, the following uses are prohibited, but not limited to: 1. Illegal activity. 2. Communication focused on commercial or for-profit purposes. 3. Communication of private/personal information of others. 4. Participation in online gaming and/or gambling. 5. Product advertisement or political lobbying. 6. Hate mail, discriminatory remarks and offensive, inflammatory, or inappropriate communication. 7. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials. 8. Access (send, receive, view, download, or transmit) to sexually suggestive, sexually explicit, obscene or pornographic material or child pornography. 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. Use of inappropriate language or profanity. 11. Transmission of material likely to be offensive or objectionable to recipients. 12. Intentional retrieval or modification of files, passwords, and data belonging to other users. 13. Impersonation of another user or communicating anonymously with the intent to harass, threaten, bully or be disrespectful to another individual. 14. Fraudulent copying/reproduction, communications, or modification of materials in violation of copyright laws.
Pol. 814	

	15. Loading or use of, or the attempt to load or use, unauthorized games, programs, files, or other electronic media. Such authorization may only be granted by a teacher or district administrator. For the security of the district's network, users should download such files only from reputable sites and only for educational purposes.
	16. Disruption of the work of other users.
	17. Destruction, modification, abuse or unauthorized access to network hardware, software and files.
	18. Quoting, summarization or other recounting of personal communications in a public forum without the original author's prior consent.
Pol. 218, 248, 252	19. Cyberbullying or any other type of harassment prohibited by law, the Student Code of Conduct, or Board Policy.
	20. Using district technology for social networking with students beyond the educational program.
	21. Texting, messaging or chatting students for any other reason than for school-related communication.
	<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 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 user's name. If a previous user has not logged off, the current user must immediately log out and then log back in under his/her own name and password.
	3. Unauthorized access, including hacking and logging into the network using another individual's username and password, is strictly prohibited and will result in discipline and denial of privileges. Such unauthorized access may also result in criminal charges.
	4. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the network.

	5. Users must create passwords that follow the guidelines for required syntax: eight (8) character minimum using a combination of numbers, letters, and special characters. 6. Users must regularly change their password when directed by district administration or state mandates. 7. User network passwords prevent unauthorized individuals from accessing the district's network without permission, however, such passwords are not required for authorized IT administrators and other district administrators to access an individual account. <u>District Email Accounts</u> The district may provide users with email accounts for the purpose of school-related communication. Use of district email accounts for personal, nonschool-related purposes is prohibited with the exception of incidental use as described in the Authority section above. The district reserves the right to revoke permission to use a district email account at any time for any reason. Users are expected to utilize email accounts in an appropriate manner and in a manner that is mindful of the personal and network security risks. Students may not send personal information to unknown individuals or individuals that they have met online. Users should not attempt to open files or follow links from unknown or untrusted origins. Users should use appropriate language. Students are prohibited from communicating via email in a manner that violates the Code of Conduct, district policy or the rules/requirements of an individual teacher. Email usage may be monitored and archived. Users are reminded that they have no expectation of privacy with regards to emails created/received on the district's system. For safety reasons, the district may periodically conduct searches of district email accounts. The district has sole discretion to access, maintain and/or destroy emails sent and/or received from a district account as it deems necessary/appropriate. <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 copyright violations and theft of services will be reported to the appropriate legal authorities for possible prosecution.
24 P.S. Sec. 4604	

	General rules for behavior and communications apply when using the Internet, district technologies, and social networking sites, in addition to the stipulations of this policy. Consequences for inappropriate use will be determined as per the District Code of Conduct or appropriate District Policies and Contracts.
	Vandalism will result in cancellation of access privileges. **Vandalism** is defined as any malicious attempt to harm or destroy data of another user. This includes but is not limited to uploading or creating computer viruses.
	<u>Copyright And Plagiarism</u>
	Federal laws, cases and guidelines will govern the use of material accessed through the district network.
	District guidelines on plagiarism, as well as the Student Code of Conduct, will govern the use of material accessed through the district network. The district's guidelines on plagiarism can be found in student handbooks. Teachers will instruct students in appropriate research and citation practices.
	<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, email, and other forms of electronic communication.
	Any district computer/server utilized by students and staff shall be equipped with Internet blocking/filtering software.
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.
	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. Prevention of unauthorized disclosure, use, and dissemination of personal information regarding minors.

5. Restriction of minor's access to materials harmful to them.

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, 104, 218, 218.2, 220, 233, 237, 248, 252, 317, 348, 417, 448, 517, 548, 814