SALISBURY TOWNSHIP SCHOOL DISTRICT

SECTION: OPERATIONS

TITLE: ACCEPTABLE USE OF TECHNOLOGY AND THE INTERNET

ADOPTED: April 17, 1996

REVISED: June 17, 2015

815. ACCEPTABLE USE OF TECHNOLOGY AND THE INTERNET

1. Purpose

The Salisbury Township 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.

This policy shall apply to all use of district Technology, including the use of district's Network. It shall also apply to all Technology used by students on school grounds, during school-sponsored activities and all Technology used by employees of the district when using such Technology on school grounds, during school-sponsored activities, at any time during their professional duties, or when representing themselves, via such Technology, as staff members or representatives of the district.

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

Guidelines for acceptable use during work hours extend to use of District-Owned Technology after work hours and/or all use of the district's Network from off-campus sites through remote login procedures.

Acceptable use of the district Network and District-Owned 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. <u>Privacy:</u> 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 as well as monitor and allocate fileserver space and access all user files. Users of District-Owned Technology have no expectation of privacy and such devices, including internet access and access histories. The district may confiscate and/or search District-Owned Technology at any time. <u>Education Related Purposes only</u>**:** For Users, the district's Network must be used for education-related purposes and performance of district job duties. Personal and/or recreational use of the internet is not permitted. Education-related purposes include 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 Salisbury Township School District establishes that Network use is a privilege, not a right. The Network and District-Owned Technology, as well as the user accounts and information, are the property of the district. Inappropriate, unauthorized and illegal use of the Network and/or District-Owned Technology 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 and/or District-Owned Technology.
3. Definitions 18 U.S.C. Sec. 2256	**Child Pornography** - under federal law, this term means 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, the term means 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. For purposes of this Policy, Child Pornography includes materials/content that meets either the Pennsylvania or federal standard or both. **Technology** - includes any district-owned, leased or licensed or user-owned personal 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, notebook, PowerBook, tablet PC or laptop computers, printers, 3D printers, cables, modems, and other peripherals including thumb and flash drives, specialized electronic equipment used for students' special educational purposes, global position system (GPS) equipment, personal digital assistants (PDAs), cell phones, with or without Internet access and/or recording and/or camera/video and other capabilities, mobile phones, or wireless devices, two-way radios/telephones, beepers, paging devices, laser pointers and attachments, and any other such technology developed. **District-owned Technology –** includes any Technology (as defined above) that is owned, leased or licensed by the District.
20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254	**Harmful to Minors** - under federal law, this term means 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, this term means 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. For purposes of this Policy, "harmful to minors" includes material/content that meets either the Pennsylvania or federal standard or both.
20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254	**Minor** - for purposes of compliance with the Children's Internet Protection Act ("CIPA"), this term means 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. Any District-Owned Technology used during the school/work day or used off district property shall be considered part of the district's Network.
47 U.S.C. Sec. 151	**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. For purposes of this Policy, "Obscene" includes material/content that meets either the Pennsylvania or federal standard or both.
18 U.S.C. Sec. 2246 18 Pa. C.S.A. Sec. 5903	**Sexual Act and Sexual Contact** – This term shall be interpreted consistent with 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 Web sites, online discussion forums, chatrooms and other social spaces online. For the purposes of this policy, **Social Networking Sites** shall also include blogs. **Blog** is a web site 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.
18 U.S.C. Sec. 1460 18 U.S.C. Sec. 2256	**Visual Depictions** – This term includes undeveloped film and videotape and data stored on computer disk or by electronic means which is capable of conversion into a visual image, that has been transmitted by any means whether or not stored in a permanent format, 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, Technology, the Internet, e-mail, 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 the Network Specialist, the Director of Data and Technology 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.
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 Technology 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. In such instances, a building administrator or designee must be present during the entire period of unrestricted research. 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. <u>Student Training</u>**:** 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 and Technology. This includes educating Minors about appropriate online behavior, including interacting with other individuals on social networking web sites and in chat rooms and cyberbullying awareness and response. 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.

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 Technology and the policies governing their use.

A copy of this policy shall be posted on the district's web site, published in the annual student handbook and available directly from the Office of the Superintendent.

Parental Notification And Responsibility

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 Network systems or Technology 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 Network systems or Technology. The district shall not be responsible for any damage users may suffer, including but not limited to, harm to persons or information that may be lost, damaged, delayed, misdelivered, or unavailable when using the Network and Technology. 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 Network systems or Technology. 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 Network systems or Technology. Salisbury Township 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 Superintendent 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 Technology is 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 by the Board. 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, PDAs and other Technology, 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. <u>Prohibitions</u> Students and employees are expected to act in a responsible, ethical and legal manner in accordance with district policy, accepted rules of network etiquette,

Pol. 814	federal and state law, the Code of Professional Practice and Ethics, and the Public School Code. Specifically, the following uses are prohibited, but are not limited to: 1. Illegal activity. 2. Communication focused on non-District-related 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, copying/reproduction, modification or use of copyrighted materials in violation of copyright laws. 8. Access (send, receive, view, download) and/or disseminate sexually suggestive, sexually explicit, Obscene, 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 use, retrieval or modification of files, passwords, and data belonging to other users. 13. Impersonation of another user (fictional or otherwise) or communicating anonymously. 14. Loading or use of unauthorized games, programs, files, or other electronic media. 15. Disruption of the work/programs/work product of other users. 16. Destruction, modification, abuse or unauthorized access to Network hardware, software and files.

	17. Quoting, summarization or other recounting of personal communications in a public forum without the original author's prior consent.
SC 1303.1-A Pol. 249	18. Cyberbullying or any other type of harassment prohibited by law, the Student Code of Conduct, or Board policy.
	19. Using District-Owned Technology for social networking with students beyond the district program.
	20. Texting students for any other reason than for school-related communication.
	21. Audio recording, video recording or photographing of a class/lesson/lecture is prohibited without the verbal permission of the teacher, administrator, or presenter.
	22. Personal hotspot use is prohibited on school grounds.
	23. Downloading or attempting to download programs over the Network or onto District-Owned Technology without express permission from IT staff, if an employee, or from a teacher or building administrator, if a student.
	24. Disseminating personally identifiable information of a student.
	25. Cyber-bullying.
	This is not intended to be an exhaustive list. Users should use their own good judgment when using the Network or District-Owned Technology.
	Examples of Acceptable use: Users should: • Use Internet, Network and Technology and online sites in a courteous and respectful manner. • Recognize that among the valuable content online, there is also content unverified, incorrect or inappropriate. Users should use trusted sources when conducting research via the Internet. • Use District Network and Technology for school-related activities. • Follow the same rules for respectful, responsible behavior online that are expected for offline behavior. • Treat school resources carefully and alert staff if there is any problem with their operation. • Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies. • Alert a teacher or other staff member of any threatening, inappropriate or harmful content (images, messages and posts) online.

- Use Network and Technology at appropriate times, in approved places, for educational pursuits.
- Cite sources when using online sites and resources for research.
- Recognize that use of Network and Technology is a privilege and treat it as such.
- Be cautious to protect the safety of themselves and others.
- Help to protect the security of school resources.

Security

Users are expected to take reasonable safeguards against the transmission of security threats over the school Network. This includes not opening or distributing infected files or programs and not opening files or programs of unknown or untrusted origin. If a user believes or suspects that a computer or device he/she is using might be infected with a virus, the user must immediately alert IT, if an employee, or his or her teacher, if a student. Users should never attempt to remove the virus themselves or download any programs to help remove the virus.

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. Users 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. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the Network.

4. Users must create passwords that follow the guidelines for required syntax: six (6) character minimum using a combination of numbers and letters.

The District will regularly review the security of the system and mandate or recommend, at regular intervals and where a potential security threat is posed, that Users change their passwords.

Consequences For Inappropriate Use

24 P.S. Sec. 4604

The Network user shall be responsible for damages to the Network and District-Owned Technology resulting from deliberate or willful acts. The District reserves the right to hold students and/or employees responsible for damage that occurs due to negligence.

Consequences of violation of this Policy may include

- Temporary or permanent suspension of Network or Technology privileges;
- Student disciplinary action, which could include detention, suspension from school-related activities, suspension from school and/or expulsion;
- Parental notification of student misuse/violation;
- Reporting of suspected illegal action to the appropriate legal authorities for possible prosecution.
- Employment disciplinary action for employee violation/misuse; and
- Legal action and/or prosecution.

Vandalism will result in cancellation of user 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.

Intentional deletion or damage to files of data belonging to others, copyright violations and theft of services shall be reported to the appropriate legal authorities for possible criminal prosecution.

<u>Employee Use Of Social Networking Media</u>

While the district understands the value of current social networking tools, it strongly discourages employees from developing virtual relationships with students through social networking tools beyond the district program. The use of district Network and/or District-owned Technology for social networking with students beyond the district program and outside of the requirements of this policy is prohibited.

All personal communications with students must be of a professional nature. Faculty/staff members must maintain strict professional boundaries of communication with students. Faculty/staff members are encouraged not to "friend" students, allow students access to the employee's non-public personal pages, or use social networking media to enter into communications with students. The district takes personal/professional boundary limits with students very seriously and may take disciplinary action against any faculty or staff member who violates this policy and/or who initiates or maintains inappropriate personal communications and/or a personal relationship with a student through any means, including social networking.

The district recommends that faculty and staff take all necessary steps to limit access to their personal social networking media and prevent students from obtaining such access. Faculty/staff members are reminded that, due to the nature of the technology, individuals do not have an expectation of privacy on social media sites.

	Faculty/Staff Members May Not: • Utilize <u>personal</u> social media sites to communicate with students for educational purposes; • Enter into inappropriate communications/relationships with students via personal social media websites or other electronic means; • Post or share on a public site or site to which students have access information that discusses or portrays sex, nudity, alcohol or drug use or other behaviors associated with the staff member's private life that would be inappropriate to discuss with a student at school; • Post or share information about identifiable students on any site, personal or professional without prior parental notification. • Disclose personally identifiable information about co-workers or supervisors on any site, personal or professional without prior written permission. • Suggest in any personal social networking context that the employee/faculty member in any way represents the district or is speaking on behalf of the district; or • Post or share discriminatory or defamatory information, or otherwise violate any district policy, including the district's policies on discrimination, harassment, privacy, and bullying on a social media site. <u>Restrictions On Social Media As An Educational Tool</u> Teachers are not permitted to require a student's use of social media within the educational program. <u>Student Use of Social media:</u> Students are prohibited from using social media, as defined in this Policy, on the District's Network during school hours and/or during school-sponsored activities. The district reserves the right to develop District-owned or sponsored social media sites for student use. In such case, the district shall develop a Student Use of Social media policy, which shall be in effect prior to a District-wide sanctioning of student use of social media and which shall govern student use of social media while at school, on District-Owned Technology and/or at school events. <u>Copyright</u>
Pol. 814	Federal laws, cases and guidelines will govern the use of material accessed through the district Network. <u>Plagiarism:</u> 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 each school's student handbook. 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, e-mail, 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.
SC 1303.1-A 47 U.S.C. Sec. 254 Pol. 249	<u>Internet Safety Programs</u> The district Administration shall assure 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.
	<u>District Email Accounts:</u> The district provides users with email accounts for the purpose of school-related communication. Use of district email accounts for personal, non-school related purposes is prohibited. 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 individual(s) 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 Network. 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 or appropriate.

Board members may be issued district email accounts. District monitoring and searches, as set forth in this Policy, shall not apply to these accounts. Where the district has reason to suspect unlawful activity occurring through the use of a Board member's email account, it shall be immediately reported to the Superintendent, who shall make a determination regarding what action is necessary, including potential referral to law enforcement. Credible suspicions of unlawful activity by Board members shall always be referred to law enforcement. The Superintendent shall contact the district Solicitor prior to taking any action regarding a Board member's email account.

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, 248, 249, 348, 448, 548, 814