ST. MARYS AREA SCHOOL DISTRICT

SECTION: OPERATIONS

TITLE: ACCEPTABLE USE OF INTERNET, COMPUTERS AND NETWORK RESOURCES

ADOPTED: November 8, 2010

REVISED: May 10, 2012

REVISED: September 14, 2015

815. ACCEPTABLE USE OF INTERNET, COMPUTERS AND NETWORK RESOURCES

1. Purpose

The Board supports use of the computers, Internet and other network resources in the district's instructional and operational programs in order to facilitate learning, teaching and daily operations through interpersonal communications and access to information, research and collaboration.

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

The use of the District's technology resources is for appropriate school-related educational and operational purposes and for the performance of job duties consistent with the educational mission of the District. Use for educational purposes is defined as use that is consistent with the curriculum adopted by the District as well as the varied instructional needs, learning styles, abilities and developmental levels of students. All use for any purpose must comply with this policy and all other applicable codes of conduct, policies, procedures, and rules and must not cause damage to the District's technology resources.

All employees and students are responsible for the appropriate and lawful use of the District's technology resources. This policy is intended to ensure that all users continue to enjoy access to the District's technology resources and that such resources are utilized in an appropriate manner and for legitimate purposes.

2. Definitions

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

18 U.S.C. Sec. 2256

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

1. The production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;
2. Such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or
3. Such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

18 Pa. C.S.A.

Sec. 6312	**Child pornography** - under state law, is any book, magazine, pamphlet, slide, photograph, film, videotape, computer depiction or other material depicting a child under the age of eighteen (18) years engaging in a prohibited sexual act or in the simulation of such act. The term harmful to minors is defined under both federal and state law.
20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254	**Harmful to minors** - under federal law, is any picture, image, graphic image file or other visual depiction that: 1. Taken as a whole, with respect to minors, appeals to a prurient interest in nudity, sex or excretion; 2. Depicts, describes or represents in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or lewd exhibition of the genitals; and 3. Taken as a whole lacks serious literary, artistic, political or scientific value as to minors.
18 Pa. C.S.A. Sec. 5903	**Harmful to minors** - under state law, is any depiction or representation in whatever form, of nudity, sexual conduct, sexual excitement, or sadomasochistic abuse, when it: 1. Predominantly appeals to the prurient, shameful, or morbid interest of minors; 2. Is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable for minors; and 3. Taken as a whole lacks serious literary, artistic, political, educational or scientific value for minors.
18 Pa. C.S.A. Sec. 5903	**Obscene** - any material or performance, if: 1. The average person applying contemporary community standards would find that the subject matter taken as a whole appeals to the prurient interest; 2. The subject matter depicts or describes in a patently offensive way, sexual conduct described in the law to be obscene; and **3.** The subject matter, taken as a whole, lacks serious literary, artistic, political, educational or scientific value.
47 U.S.C. Sec. 254	**Technology protection measure** - a specific technology that blocks or filters Internet access to visual depictions that are obscene, child pornography or harmful to minors. District technology resources means all technology owned and/or operated by the District, including computers, projectors, televisions, video and sound systems, mobile devices, calculators, scanners, printers, cameras, portable hard drives, hardware, software, routers, and networks, including the Internet. User means anyone who utilizes or attempts to utilize District technology resources while on or off District property. The term includes, but is not limited to, students, staff, parents and/or guardians, and any visitors to the District that may use District technology.

3. Authority	The availability of access to electronic information does not imply endorsement by the district of the content, nor does the district guarantee the accuracy of information received. The district shall not be responsible for any information that may be lost, damaged or unavailable when using the network or for any information that is retrieved via the Internet. The district shall not be responsible for any unauthorized charges or fees resulting from access to the Internet or other network resources.
Pol. 218, 233, 317	The Board declares that computer and network use is a privilege, not a right. The district's computer and network resources are the property of the district. Users shall have no expectation of privacy in anything they create, store, send, receive or display on or over the district's Internet, computers or network resources, including personal files or any use of the district's Internet, computers or network resources. The district reserves the right to monitor, track, and log network access and use; monitor fileserver space utilization by district users; or deny access to prevent unauthorized, inappropriate or illegal activity and may revoke access privileges and/or administer appropriate disciplinary action. The district shall cooperate to the extent legally required with the ISP, local, state and federal officials in any investigation concerning or related to the misuse of the district's Internet, computers and network resources. The Superintendent or his/her designee is ultimately responsible for overseeing the District's technology resources. The Superintendent will designate a network administrator who will serve as the coordinator and supervisor of the District's technology resources and networks, and who will work with other regional and state organizations as necessary to educate users, approve activities, provide leadership for proper training for all users in the use of District's technology resources and the requirements of this policy, and who will establish a system to ensure that users who access District technology resources have agreed to abide by the terms of this policy. The Board requires all users to fully comply with this policy and to immediately report any violations or suspicious activities to the Superintendent or designee.
47 U.S.C. Sec. 254 Pol. 103, 103.1, 104, 248, 348 Pol. 249	The Board establishes the following materials, in addition to those stated in law and defined in this policy, that are inappropriate for access by minors: 1. Defamatory. 2. Lewd, vulgar, or profane. 3. Threatening. 4. Harassing or discriminatory. 5. Bullying.
24 P.S. Sec. 4604 20 U.S.C. Sec. 6777 47 U.S.C.	The district reserves the right to restrict access to any Internet sites or functions it deems inappropriate through established Board policy, or the use of software and/or online server blocking. Specifically, the district operates and enforces a technology protection measure(s) that blocks or filters access to inappropriate matter by minors on its computers used and accessible to adults and students. The technology protection measure shall be enforced during use of computers with Internet access.

Sec. 254 24 P.S. Sec. 4604 24 P.S. Sec. 4610 20 U.S.C. Sec. 6777	Upon request by students or staff, the Superintendent or designee shall expedite a review and may authorize the disabling of Internet blocking/filtering software to enable access to material that is blocked through technology protection measures but is not prohibited by this policy. Upon request by students or staff, building administrators may authorize the temporary disabling of Internet blocking/filtering software to enable access for bona fide research or for other lawful purposes. Written permission from the parent/guardian is required prior to disabling Internet blocking/filtering software for a student's use. If a request for temporary disabling of Internet blocking/filtering software is denied, the requesting student or staff member may appeal the denial to the Superintendent or designee for expedited review.
4. Delegation of Responsibility 24 P.S. Sec. 4604	The Superintendent or designee shall develop procedures, in cooperation with the District technology staff, for the acceptable use of all District technology resources including, but not limited to: software, hardware, electronic devices, servers, and networks. The district shall make every effort to ensure that this resource is used responsibly by students and staff. The district shall inform staff, students, parents/guardians and other users about this policy through employee and student handbooks, posting on the district web site, and by other appropriate methods. A copy of this policy shall be provided to parents/guardians, upon written request. Users of district networks or district-owned equipment shall, prior to being given access or being issued equipment, sign user agreements acknowledging awareness of the provisions of this policy, and awareness that the district uses monitoring systems to monitor and detect inappropriate use and tracking systems to track and recover lost or stolen equipment. Student user agreements shall also be signed by a parent/guardian. Administrators, teachers and staff have a professional responsibility to work together to help students develop the intellectual skills necessary to discern among information sources, to identify information appropriate to their age and developmental levels, and to evaluate and use the information to meet their educational goals. Students, staff and other authorized individuals have the responsibility to respect and protect the rights of every other user in the district and on the Internet. Building administrators shall make initial determinations of whether inappropriate use has occurred.
20 U.S.C. Sec. 6777 47 U.S.C.Sec. 254 47 CFR	The Superintendent or designee shall be responsible for recommending technology and developing procedures used to determine whether the district's computers are being used for purposes prohibited by law or for accessing sexually explicit materials. The procedures shall include but not be limited to:

Sec. 54.520	1. Utilizing a technology protection measure that blocks or filters Internet access for minors and adults to certain visual depictions that are obscene, child pornography, harmful to minors with respect to use by minors, or determined inappropriate for use by minors by the Board. 2. Maintaining and securing a usage log. 3. Monitoring online activities of minors.
47 U.S.C. Sec. 254 SC 1303.1-A Pol. 249	The Superintendent or designee shall develop and implement administrative regulations that ensure students are educated on network etiquette and other appropriate online behavior, including: 1. Interaction with other individuals on social networking web sites and in chat rooms. 2. Cyberbullying awareness and response.
5. Guidelines	Network accounts shall be used only by the authorized owner of the account for its approved purpose. The authorized owner of the account will receive or create a password of a minimum of eight characters and include alpha, numeric, and special characters. Network users shall respect the privacy of other users on the system. <u>Safety</u> It is the district's goal to protect users of the network from harassment and unwanted or unsolicited electronic communications. Any network user who receives threatening or unwelcome electronic communications or inadvertently visits or accesses an inappropriate site shall report such immediately to a teacher or administrator. Network users shall not reveal personal information to other users on the network, including chat rooms, e-mail, social networking web sites, etc. <u>Unauthorized Use Prohibited</u> Only users who have agreed to abide by the terms of this policy may utilize the District's technology resources. Unauthorized use, utilizing another user's District account, or exceeding one's authorization to use District technology resources is prohibited. <u>Use of Personal Electronic Devices</u> The use of personal electronic devices on the District network is permitted only on designated networks. When a user connects a personal electronic device to a District network or District technology resources, this policy and its guidelines apply. Users are subject to the same levels of monitoring and access as if a District-owned device were being utilized. Users who connect a personal electronic device to a District network explicitly waive any expectation of privacy in the content exchanged over the District technology resources. <u>Privacy</u> The District reserves the right to monitor any user's utilization of District technology resources. Users have no expectation of privacy while using District technology resources whether on or off District property. The District may monitor, inspect, copy, and review any and all usage of District technology resources including

	information transmitted and received via the Internet to ensure compliance with this and other District policies, and state and federal law. All emails and messages, as well as any files stored on District technology resources may be inspected at any time for any reason.
Children's Internet Protection Act 47 U.S.C 254 34 C.F.R. 54.520 Child Internet Protection Act 24 P.S. 4601 et seq.	<u>Internet Filtering and CIPA Compliance</u> The District utilizes content and message filters to prevent users from accessing material through District technology resources that has been determined to be obscene, offensive, pornographic, harmful to minors, or otherwise inconsistent with the District's educational mission. The Superintendent or his/her designee shall establish a procedure for users to request that a legitimate website or educational resource not be blocked by the District's filters for a bona fide educational purpose. Such requests must be either granted or rejected within three school days pursuant to the established procedure. The Board directs that the Superintendent or his/her designee ensure that students at the elementary, middle school, and high school levels are educated about appropriate online behavior including interacting via social networks and in chat rooms, cyber-bullying, and disclosure of personal information. <u>Monitoring</u> District technology resources shall be periodically monitored to ensure compliance with this and other District policies including monitoring of user's online activities. The network administrator designated by the Superintendent shall ensure that regular monitoring is completed pursuant to this section. However, the Superintendent, or his/her designee, shall also implement procedures to ensure that District technology resources are not utilized to track the whereabouts or movements of individuals, and that remotely activated cameras and/or audio are not utilized except where necessary to recover lost or stolen District technology. <u>District Provided Resources</u> The following uses of District technology resources are prohibited: 1. Use of technology resources to violate the law, facilitate illegal activity, or to encourage other to do so. 2. Use of technology resources to violate any other District policy. 3. Use of technology resources to engage in any intentional act which might threaten the health, safety, or welfare of any person or persons. 4. Use of technology resources to cause, or threaten to cause harm to others or damage to their property. 5. Use of technology resources to bully, or to communicate terroristic threats, discriminatory remarks, or hate. 6. Use of technology resources to communicate words, photos, videos, or other depictions that are obscene, indecent, vulgar, rude, profane, or that advocate illegal drug use. 7. Use of technology resources to create, access, or to distribute obscene, profane, lewd, vulgar, pornographic, harassing, or terroristic materials, firearms, or drug paraphernalia.

8. Use of technology resources to attempt to interfere with or disrupt District technology systems, networks, services, or equipment including, but not limited to, the propagation of computer "viruses" and "worms", Trojan Horse and trapdoor program codes.
9. Altering or attempting to alter other user's or system files, system security software, system or component settings, or the systems themselves, without authorization.
10. The attempted physical harm or attempted destruction of District technology resources.
11. Use of technology resources in a manner that jeopardizes the security of the District's technology resources, or in a manner that attempts to circumvent any system security measures.
12. Use of technology resources to intentionally obtain or modify files, passwords, and/or data belonging to other users or to the District.
13. Use that conceals or attempts to conceal a user's identity, including the use of anonymizers, or the impersonation of another user.
14. Unauthorized access, interference, possession, or distribution of confidential or private information.
15. Using technology resources to send any District information to another party, except in the ordinary course of business as necessary or appropriate for the advancement of the District's business or educational interests.
16. Use of technology resources to commit plagiarism.
17. Installing, loading, or running software programs, applications, or utilities not explicitly authorized by the District technology staff.
18. Installing unauthorized computer hardware, peripheral devices, network hardware, or system hardware onto technology resources.
19. Copying District software without express authorization from a member of the District's technology staff.
20. Use of technology resources for commercial purposes.
21. Use of technology resources for political lobbying or campaigning, not including student elections (e.g. student government, club officers, homecoming queen, etc.).
22. Use of District technology resources to tether or otherwise connect to a non-District owned device to access an unfiltered and/or unmonitored internet connection.
23. The use of proxies or other means to bypass internet content filters and monitoring.
24. The use of technology resources to gamble.
25. Unauthorized access into a restricted system or changing settings or access rights to a restricted system or account.
26. The use of encryption software that has not been previously approved by the District.
27. Sending unsolicited mass-email messages, also known as spam.
28. Scanning the District's technology resources for security vulnerabilities.

	Security System security is protected through the use of passwords. Failure to adequately protect or update passwords could result in unauthorized access to personal or district files. To protect the integrity of the system, these guidelines shall be followed: 1. Employees and students shall not reveal their passwords to another individual. 2. Users are not to use a computer that has been logged in under another student's or employee's name. 3. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the network.
17 U.S.C. Sec. 101 et seq Pol. 814	Copyright The illegal use of copyrighted materials is prohibited. Any data uploaded to or downloaded from the network shall be subject to fair use guidelines and applicable laws and regulations.
	District Web Site The district shall establish and maintain a web site and shall develop and modify its web pages to present information about the district under the direction of the Superintendent or designee. All users publishing content on the district web site shall comply with this and other applicable district policies. Users shall not copy or download information from the district web site and disseminate such information on unauthorized web pages without authorization from the building principal.
24 P.S. Sec. 4604	Consequences for Inappropriate Use of District Technology Violations of this policy may result in the temporary or permanent revocation of a user's right to access District technology resources. Additionally, students may be subject to other forms of disciplinary actions for violations of this plicy and/or local, state, and/or federal law. The network user shall be responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts. Illegal use of the network; intentional deletion or damage to files or data belonging to others; copyright violations; and theft of services shall be reported to the appropriate legal authorities for possible prosecution. General rules for behavior and communications apply when using the Internet, in addition to the stipulations of this policy. Vandalism shall result in loss of access privileges, disciplinary action, and/or legal proceedings. **Vandalism** is defined as any malicious attempt to harm or destroy data of another user, Internet or other networks; this includes but is not limited to uploading or creating computer viruses.

Pol. 218, 233, 317	Failure to comply with this policy or inappropriate use of the Internet, district network or computers shall result in usage restrictions, loss of access privileges, disciplinary action, and/or legal proceedings. LIMITATION OF LIABILITY: In no event shall the St. Marys Area School District be liable for damages, whether direct, indirect, special or consequential, arising out of the use of its hardware, software and network technologies. This includes any interruption of user access. References: School Code – 24 P.S. Sec. 1303.1-A PA Crimes Code – 18 Pa. C.S.A. Sec. 5903, 6312 Child Internet Protection Act – 24 P.S. Sec. 4601 et seq. U.S. Copyright Law – 17 U.S.C. Sec. 101 et seq. Sexual Exploitation and Other Abuse of Children – 18 U.S.C. Sec. 2256 Enhancing Education Through Technology Act – 20 U.S.C. Sec. 6777 Internet Safety, Children's Internet Protection Act – 47 U.S.C. Sec. 254 Children's Internet Protection Act Certifications, Title 47, Code of Federal Regulations – 47 CFR Sec. 54.520 Board Policy – 103, 103.1, 104, 218, 218.2, 220, 233, 237, 248, 249, 317, 348, 814

St. Marys Area School District
Computer Acceptable Use Policy Summary

PURPOSE:

All use of the Internet and computer network must be in support of education and research and consistent with the purposes of the St. Marys Area School District.

The Internet and computer network will be used to support the district's curriculum, the educational community, communications, research and projects between schools for district students, teachers and administrators.

AUTHORITY:

The St. Marys Area School District reserves the right to log Internet use, to monitor fileserver space utilization, to review files and communications by District users while respecting the privacy rights of both District users and outside users. The school reserves the right to remove a user account from the network to prevent further unauthorized or illegal activity.

PROCEDURES:

Only the authorized owner of the account will use network accounts for its authorized purpose. Network users shall respect the privacy of other users on the system and all communications and information accessible via the network should be assumed to be private property and shall not be disclosed except for district purposes consistent with the objectives of this and related policies. The authorized owner of the account will receive or create a password of a minimum of eight characters and include alpha, numeric and special characters. Use of St. Marys Area School District's computer hardware, software, network, Internet or email requires the signing of the user agreement form by all users. If the user is under the age of 18 or is a student living with a parent or guardian, the signature of the parent or guardian is also required. The district, at its sole discretion, may waive the signature of young users or those unable to read or fully comprehend these policies. (Parent/guardian signature is still required.)

PROHIBITIONS:

The use of the Internet and computer network for illegal, inappropriate or unethical purposes by students, employees or other authorized users is prohibited. More specifically:

- Use of the network and/or the Internet to facilitate illegal activity is prohibited.
- Use of the network and/or the Internet for commercial or for-profit purposes is prohibited.
- Use of the network and/or the Internet for non-work or non-school related communications is prohibited.
- Use of the network and/or the Internet for product advertisement or political lobbying is prohibited.
- Malicious use of the network and/or the Internet to develop programs that harass other users or infiltrate a computer system and/or damage hardware and software components of a computer or system is prohibited.
- The creation, use or sharing of computer viruses is prohibited.
- Hate mail, harassment, discriminatory remarks and other antisocial communications on the network and/or the Internet is prohibited.

- Use of the network and/or the Internet to access obscene, pornographic or socially unacceptable material is prohibited.
- Use of the network and/or the Internet to transmit material likely to be offensive or objectionable to recipients is prohibited.
- Use of the network and/or the Internet to misrepresent other users on the network and/or the Internet is prohibited.
- Use of school technology, the network and/or the Internet for fraudulent copying, communications or modification of materials in violation of law is prohibited and will be referred to appropriate authorities.
- Loading or use of unauthorized games, programs, files or other electronic media is prohibited.
- The network and/or the Internet shall not be used to disrupt the work of others; and the hardware or software of other users shall not be destroyed, modified or abused in any way.
- Use of the network and/or the Internet that results in any copyright violation is prohibited.
- All users with email must manage email accounts including the regular and frequent deletion of mail.
- A subscription to Listservers, Newsgroups or other such services without preapproval by the district is prohibited.
- All users are prohibited from creating mobile hot spots and/or any other wireless solution and connecting District-owned equipment to those hot spots and/or any other wireless solution to bypass in place web filtering solutions and wireless solutions on District property.

CONSEQUENCES:

- St. Marys Area School District may terminate the availability of the Internet and/or network at its sole discretion.
- Inappropriate Use – The network and/or the Internet user, whether student, employee or other user, shall be responsible for damages to the equipment, systems or software resulting from deliberate or willful acts.
- Failure to follow the procedures and prohibitions listed above may result in the loss of the right of access to the Internet. Other appropriate disciplinary procedures may take place, as needed, for students, employees or other authorized users.
- Illegal use of the network; intentional deletion or damage to files of data belonging to others; copyright violations or theft of services will be reported to the appropriate legal authorities for possible prosecution.

LIMITATION OF LIABILITY:

In no event shall the St. Marys Area School District be liable for damages, whether direct, indirect, special or consequential, arising out of the use of its hardware, software and network technologies. This includes any interruption of user access.

ST. MARYS SCHOOL DISTRICT USER AGREEMENT AND PERMISSION FORM

I have read, understand and accept the attached Computer Acceptable Use Policy Summary and the complete Acceptable Use of Internet, Computers and Network Resources Policy #815 available on the District webpage at www.smasd.org. These policies govern my use of technology, computer network and Internet at St. Marys Area School District. I recognize that violations may result in a loss of access as well as other disciplinary or legal action.

I also agree to comply with stated rules that may be established by the St. Marys Area School District regarding network, communication and management of the system.

User signature (full name) _____

Please print name _____

Building _____ Date _____