South Middleton School District

SECTION: OPERATIONS

TITLE: ACCEPTABLE USE POLICY FOR TECHNOLOGY

ADOPTED: November 17, 1997

REVISED: May 21, 2012

	815. ACCEPTABLE USE POLICY FOR TECHNOLOGY
1. Purpose	The Board supports use of the Internet and other computer networks in the district's instructional and operational programs in order to facilitate learning, teaching and daily operations through the interpersonal communications and access to information, research and collaboration. For instructional purposes, the use of physical and virtual network facilities shall be consistent with the curriculum adopted by the school district as well as the varied instructional needs, learning styles, abilities, and developmental levels of students.
2. Definitions 18 Pa.C.S.A. Sec. 5903 18 U.S.C. 1460 18 U.S.C. 2256 47 C.F.R. 54.520	Obscene – material which: to the average person, applying contemporary community standards, appeals to the prurient interest; depicts or describes in a patently offensive way, sexual conduct described by law to be obscene; and taken as a whole, lacks serious literary, artistic, political, educational or scientific value. Child Pornography – 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. Harmful to Minors – any picture, image, graphic image file or other visual depiction that: (1) taken as a whole and 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 a lewd exhibition of the genitals; and (3) take as a whole, lacks serious literary, artistic, political, or scientific value as to minors. The Board may establish a list of materials, in addition to those stated in law, that are deemed inappropriate for access by minors.

	Technology Protection Measure – a specific technology that blocks or filters Internet access to visual depictions that are obscene, child pornography, or, with respect to use of the computers by minors, harmful to minors.
3. Guidelines	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 shall not be responsible for any unauthorized charges or fees resulting from access to the Internet. <u>Limits of Privacy</u> The district reserves the right to log and monitor network use, computer network activity, e-mail, electronic communications and fileserver space utilization by district users, while respecting the privacy rights of both district users and outside users. All users shall have no expectation of privacy within any and all Internet use, computer network activity, email and electronic communications and files stored on district servers, computers, network appliances or other technology devices. SMSD further reserves the right to reasonably monitor and regulate the accounts of students and staff in order to ensure compliance with this entire computer use policy. This includes, but may not be limited to, physical surveillance of users as they access the network, interception of electronic messages, and investigation of network logs and activity.
.	Administrators, teachers and staff have a professional responsibility to work together to help students develop the intellectual skills necessary to discriminate among information sources, to identify information appropriate to their age and developmental levels, and to evaluate and use the information responsibly and ethically to meet their educational goals. Students and staff have the responsibility to respect and protect the rights of every other user in the district and on the Internet. The district shall make every effort to ensure that this network as a resource is used responsibly by students and staff. Building administrators shall have the authority to determine what is ‘appropriate use’, and shall report all incidents of abuse to the network administrator, in a timely manner. The District reserves the right to remove or restrict any user’s account from the network, to prevent further unauthorized or illegal activity. Use of electronic communications devices on the District network must be consistent with Policy 237 and, if applicable, the Bring Your Own Technology Agreement.

	Content Filtering and Internet Security In accordance with the requirements set forth in the Children's Internet Protection Act (CIPA) and Protecting Children in the 21st Century Act, the District enforces a policy of Internet Safety that includes monitoring online activities and the operation of technology protection measures that protect against Internet access by both adults and minors to visual depictions that are obscene, child pornography, or, with respect to use of computers by minors, harmful to minors. Even with a content filter and other technology protection measures in place, the District cannot guarantee the filter to be 100% effective. Administrators or other authorized persons may, upon receipt of a proper written request, disable technology protection measures during use by an adult to enable access for bona fide research or other lawful purpose.
20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254 47 C.F.R. § 54.520	The Superintendent or designee shall be responsible for recommending technology protection measures. The measures 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. The District will annually provide instruction to students and staff about appropriate online behavior, including interacting with individuals on social networking sites and chat rooms. The District will further provide instruction on cyber bullying awareness and the appropriate response, based on the curriculum taught at each grade level. Following receipt of training, the student will acknowledge that he/she received the training, understood it, and will follow the provisions of this policy. Security Network accounts shall be used only by the authorized owner of the account for its approved purpose. All communications and information accessible via the network should be assumed to be property of the District and subject to investigation at any time. Network users shall respect the privacy of other users on the system. Use of another person's identity to access technology and network resources is prohibited. System security is protected through the use of passwords. Failure to adequately protect or update passwords could result in unauthorized access to personal or district files. To

protect the integrity of the system, the following guidelines shall be followed:

1. Employees and students shall not reveal their passwords to another individual.

2. Users are not to use a computer that has been logged in under another student's or employee's name.

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

4. Users may not allow others to access the computer network by sharing account information or passwords.

5. Users may not move, repair, reconfigure, modify, or attach external devices to any network equipment. All malfunctions, problems, and suspected violations shall be immediately reported to District technology personnel.

6. No computer software is to be installed onto any SMSD computer by staff or students. District technology personnel will only install software that has been legally obtained through the official purchasing process of SMSD.

7. Storage media and devices not authorized by SMSD may not be inserted or connected to any SMSD computer or network device.

A computer virus is a malicious software program created for the purpose of disrupting computer systems, destroying information, and disrupting operations. These insidious invasions can cost thousands of dollars to undo. Certain safeguards are in place to protect the network, however this are no guarantees. Anyone who willfully introduces a computer virus onto the network or any equipment owned by SMSD will have their computer privileges restricted, suspended, or revoked and may be held liable for damages.

<u>Prohibitions</u>

Students and staff are expected to act in a responsible, ethical and legal manner in accordance with district policy, accepted rules of network etiquette, and federal and state law. Specifically, the following uses are prohibited:

1. Facilitating illegal activity.

2. Commercial or for-profit purposes.
3. Nonwork or nonschool related work.

4. Product advertisement, political and/or religious lobbying.

	5. Bullying/Cyberbullying. 6. Hate mail, discriminatory remarks, and offensive or inflammatory communication. 7. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials. 8. Access to obscene or pornographic material or child pornography. 9. Access by students and minors to material that is harmful to minors or it determined inappropriate for minors in accordance with Board policy. 10. Inappropriate language or profanity. 11. Transmission of material likely to be offensive or objectionable to recipients. 12. Intentionally obtaining or modifying of files, passwords, and data belonging to other users. 13. Impersonation of another user, anonymity, and pseudonyms. 14. Fraudulent copying, communications, or modification of materials in violation of copyright laws. 15. Loading or using of unauthorized games, programs, files or other electronic media. 16. Disruption of the work of other users. 17. Destruction, modification, abuse or unauthorized access to network hardware, software and files. 18. Quoting of personal communications in a public forum without the original author's prior consent. 19. Use of wireless, unfiltered connection to the Internet during the school day, on school property, and during any school-sponsored activities. The District will provide filtered, authenticated, wireless access to the Internet for student and staff use. 20. Use of the computer network for sending frivolous electronic mail (e-mail), chatting, reading and sending jokes, researching nonwork and nonschool related work, and playing computer games.

21. Vandalism- defined as: any malicious attempt to harm or destroy district/network equipment, data of another user, Internet, or other networks, including but not limited to uploading or creating malicious code and computer viruses; physical destruction of computer equipment; destruction of cabling and network infrastructure; attempts to gain unauthorized access by defeating network security (commonly known as "hacking"); and attempts to gain access by using a different account or password and destruction or alteration of files.

22. Use of the system for defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, offensive, and illegal material.

Consequences For Inappropriate Use

The Board establishes that network use is a privilege, not a right. Violations of this Policy will result in limitation or cancellation of those privileges and appropriate disciplinary action.

Violations of this policy by a student shall result in disciplinary action, including the range of penalties provided for in the Student Code of Conduct and Student Handbook.

Violations of this policy by an employee shall result in disciplinary action up to and including discharge.

The network user shall be responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts.

PRIVACY

For the protection of our students, all users are advised and should be reinforced by parents/ guardians to NEVER disclose personal information over the network such as home address, physical description, route to and from school, or any other personal information that could threaten the safety and security of our children.

Copyright

Software copyright violations will not be tolerated and proper software licensing will be aggressively enforced by SMSD. The district Software Compatibility form shall be completed and submitted for approval before software is purchased or installed. Any question or concern about the legality of software should be referred to the SMSD administration.

	Acceptable Use Policy – Student Consent Form Acceptable Use Policy – Faculty/Staff Consent Form Acceptable Use Policy – Adult/Guest Computer User Consent Form