SPRING GROVE AREA SCHOOL DISTRICT

SECTION: OPERATIONS

TITLE: RESPONSIBLE USE OF INTERNET AND NETWORK RESOURCES

ADOPTED: November 20, 1996

REVISED: February 22, 2016

815. RESPONSIBLE USE OF INTERNET AND NETWORK RESOURCES

1. Purpose

Spring Grove Area School District provides all users access to technology tools and Internet resources as part of the district's core educational mission and goals. Technology permeates virtually all district academic activities, operations, communications and research. It is the intent of Spring Grove Area School District to promote responsible, ethical and appropriate use of technology and network resources.

The purpose of this policy is to outline expectations for acceptable and responsible use of district technology resources by students, staff and the community ("all users"). For purposes of this policy, **technology resources** includes but is not limited to any school district-owned, leased or licensed or user-owned personal hardware, software, or other technology, including cell phones and personal electronic devices, used on school district premises or at school district events. Access to district technology and network resources is a privilege, not a right. All users will be held accountable for noncompliance with this policy.

2. Definitions
18 Pa. C.S.A. Sec. 5903

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.

18 U.S.C. Sec. 2256

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.

20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254	**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) taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.
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, with respect to use of the computers by minors, harmful to minors.
3. Authority	The electronic information available to all users does not imply endorsement by the district of the content, nor does the district guarantee the accuracy of information received. The district will 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 will not be responsible for any unauthorized charges or fees resulting from access to the Internet. Costs associated with the use of data and applications on personal electronic devices will be the responsibility of the user. The district reserves the right to log and monitor Internet use, computer network activity, e-mail, electronic communications and file server space utilization by all users. District administration or a designee may review user files and communications to maintain system integrity and ensure that all users are using the system responsibly. All users will 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. The district reserves the right to remove or restrict a user account from the network to prevent further unauthorized or illegal activity.
4. Delegation of Responsibility	All users have the responsibility to respect and protect the rights of every other network user in the district and on the Internet. District staff have a professional responsibility to help students develop skills necessary to evaluate information sources, identify age-appropriate information and utilize online media resources to meet educational goals.
24 P.S. Sec. 4604	The district will inform staff, students, parents/guardians and other users about this policy through employee and student handbooks, posting on the district website, and by other appropriate methods. A copy of this policy will be provided to parents/guardians, upon written request.

Pol. 237	Per district policy 237, the use of personal electronic devices is permitted on district-designated networks only. All use of personal electronic devices must be in accordance with district policy 237. All users who connect to permitted networks agree to the requirements of this Responsible Use of Internet and Network Resources policy and should consider his/her personal device subject to the same level of monitoring and access as any district-owned electronic device. The district reserves the right to monitor Internet and network use on district guest networks.
5. Guidelines	<u>Responsible and Acceptable Use</u> All users are expected to act in a professional, responsible, ethical and legal manner when utilizing district technology, network and Internet resources. Users must read, understand, provide a signed acknowledgment form and comply with this policy, which includes: 1. Use of the Internet and network resources must be in support of district educational and operational programs. 2. Illegal activity, commercial activities, lobbying, and unauthorized advertising are prohibited. 3. Hate mail, discriminating remarks, profanity, inappropriate language and offensive communications are prohibited.
SC 1303.1-A Pol. 248, 249	4. Bullying, cyberbullying and harassment are prohibited. The student will abide by district bullying policies when utilizing district technology, network and Internet resources. 5. Access to or distribution of pornographic, obscene, lewd, illegal or other material deemed harmful to minors is prohibited. 6. Users will not intentionally seek information on, modify, or obtain copies of files, other data, or passwords belonging to other users, or misrepresent other users on the network.
Pol. 814	7. Use of school technology or network connectivity for fraudulent or illegal copying, communication, taking or modification of material in violation of law is prohibited and will be referred to appropriate authorities. 8. Loading, distribution, or use of unauthorized software, programs or utilities on district technology or network services without prior approval from the district Technology Coordinator or his/her designee is strictly prohibited.

Pol. 814	9. All users are expected to adhere to copyright laws and regulations. The illegal use of copyrighted software, materials, or files is prohibited. 10. The network will not be used to disrupt the work of others; hardware or software will not be destroyed, modified or abused in any way.
24 P.S. Sec. 4604	11. All users will be responsible for damages to equipment, systems and software resulting from deliberate or willful acts. Users will not be responsible for damage due to normal wear and tear or for accidental damage, loss, or theft. 12. Any attempt to circumvent security measures on the district network or technology devices is prohibited. Unauthorized access, deletion or modification of passwords, files and data belonging to other users is prohibited. All users should report any security problems to the school administration.
Pol. 237	13. Laser pointers and other laser-emitting devices are strictly prohibited.
20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254 47 CFR Sec. 54.520	<u>Content Filtering and Internet Safety</u> In accordance with the requirements set forth by the United States Congress in the Children's Internet Protection Act (CIPA) and Protecting Children in the 21st Century Act, Spring Grove Area School 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.
SC 1303.1-A 47 U.S.C. Sec. 254 Pol. 249	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 cyberbullying awareness and the appropriate response, based on the curriculum taught at each grade level. Following receipt of this training, the student will acknowledge that he/she received the training, understood it, and will follow the provisions of this policy.

Security

All users are expected to act responsibly and protect the integrity and security of district data, passwords and user-identity. All users are expected to keep passwords and other digital security credentials confidential. Users should not attempt to gain access to unauthorized systems. Use of another person's identity to access technology and network resources is prohibited. Users may not distribute malware, viruses, or any other grayware applications. Users are also prohibited from hacking into the network or others' computers by exploiting the network or devices. This includes but is not limited to, using a vulnerability scanner, password cracking, packet sniffers, spoofing attacks, rootkits, or social engineering attacks. Any applications used to strip or harvest information from the network or district-owned computers, completely take over a person's computer, or to "look around," is strictly prohibited.

Parental Notification and Responsibility for District-owned Devices Used Outside of the District Network

There is a wide range of material available on the Internet, some of which may not be consistent with the particular values of families of the students. While the devices given to students are integral to completing coursework beyond the school day, it is not practically possible for the district to monitor, filter, and enforce a wide range of social values in student use of the Internet when those devices are taken and used outside of the district network. Further, the district recognizes that parents/guardians maintain primary responsibility for transmitting their particular set of values to their children. The district encourages parents/guardians to discuss and specify to their child(ren) what material is and is not acceptable for their child(ren) to access on personal devices through the Internet, based upon the set of social values specific to each family.

Disclaimer

Spring Grove Area School District makes no warranties of any kind, whether express or implied, for the network or technology services provided. The district is not responsible for any damages incurred, including loss of data resulting from data delivery delays, missed deliveries, or financial obligations incurred through the use of Internet web sites. Use of any information obtained through the district's technology devices is at the user's risk. The district disclaims responsibility for the accuracy or quality of information obtained through the Internet or other forms of electronic communication.

Pol. 218, 233, 317, 417, 517	Consequences for Inappropriate Use General rules for behavior, ethics, and communications apply when using the network, internet and related resources and information, in addition to the stipulations of this policy. Users must be aware that violations of this policy or other policies, or for unlawful use may result in loss of network access and a variety of other disciplinary actions, including, but not limited to, warnings, usage restrictions, loss of privileges, position reassignment, oral or written reprimands, suspensions (with or without pay for employees), dismissal, expulsions, and/or legal proceedings on a case-by-case basis. This policy incorporates all other relevant district policies, such as, but not limited to, the student, administrative, professional, and classified employee handbooks, the district's professional code of conduct policy, discipline policies, copyright policy, property policies, curriculum policies, terroristic threat policy and harassment policies, as well as the electronic devices policy. Violations as described in this policy may be reported to the school district, appropriate legal authorities, whether the Internet Service Provider, local, state, or federal law enforcement. The school district will cooperate to the extent legally required with authorities in all such investigations.

References:

School Code – 24 P.S. Sec. 510, 1303.1-A, 1317.1

State Board of Education Regulations – 22 Pa. Code 403.1

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

Protecting Children in the 21st Century Act – 15 U.S.C. Sec. 6551

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, 249, 317, 348, 417, 448, 517, 548, 814