SPRING-FORD AREA SCHOOL DISTRICT

SECTION: OPERATIONS

TITLE: ACCEPTABLE USE OF THE ELECTRONIC COMMUNICATIONS SYSTEMS

ADOPTED: January 26, 1998

REVISED: June 24, 2019

815. ACCEPTABLE USE OF THE ELECTRONIC COMMUNICATIONS SYSTEMS

1. Purpose

The Spring-Ford Area School District (school district) provides employees, students, and guests (users) access to technology resources including, but not limited to, electronic communications systems, computers, computer networks, networked devices, hardware, software, internet access, mobile devices, peripherals, copiers, and cameras.

The Board of School Directors supports the use of the district's technology resources to facilitate teaching and learning, to provide access to information, to aid in research and collaboration, to foster the educational mission of the district, and to carry out the legitimate business and operation of the district.

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 have access to the district's technology resources and that such resources are utilized in an appropriate manner and for legitimate purposes.

The school district intends to strictly protect its district technology resources against numerous outside and internal risks and vulnerabilities. Users are important and critical players in protecting these school district assets and in lessening the risks that can destroy these important and critical assets. Consequently, users are required to

	fully comply with this policy, and to immediately report any violations or suspicious activities to the Director of Technology and/or designee through their supervisor or teacher. Conduct otherwise will result in actions further described below in Consequences **for** Inappropriate, Unauthorized **and** Illegal Use, found in the last section of this policy, and provided in relevant school district policies.
2. Definitions 18 U.S.C. Sec. 2256	**Child Pornography** - under federal law, any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where: 1. The production of such visual depiction involves the use of a minor engaging in sexually explicit conduct. 2. Such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct. 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, **child pornography** includes 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. **District Technology Resources** - includes any school district-owned, leased or licensed or user-owned personal hardware, software, or other technology used on school district premises or at school district events, or connected to the school district network, containing school district programs or school district or student data (including images, files, and other information) attached or connected to, installed in, or otherwise used in connection with a computer. District technology resources includes, but is not limited to, school district and users': desktop, notebook, tablet, PC or laptop computers, printers, facsimile machine, cables, modems, and other peripherals; specialized electronic equipment used for students' special educational purposes; global positioning system (GPS) equipment; 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; laser pointers and attachments; and any other such technology developed. **Electronic Communications Systems** - any messaging, collaboration, publishing, broadcast, or distribution system that depends on electronic communications resources to create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, or print electronic records for purposes of communication across electronic communications network systems between or among individuals or

	groups, that is either explicitly denoted as a system for electronic communications or is implicitly used for such purposes. Further, an electronic communications system means any wire, radio, electromagnetic, photo optical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications. Examples include, but are not limited to, the Internet, intranet, electronic mail services, global positioning systems, personal digital assistants, facsimile machines, cell phones with or without Internet access and/or electronic mail and/or recording devices, cameras/video, and other capabilities. **Educational purpose** - includes use of the district technology resources for classroom activities, professional or career development, and to support the school district's curriculum, policy and mission statement.
20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254	**Harmful to Minors** - under federal law, any picture, image, graphic image file or other visual depictions that: 1. 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, the term includes 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.
47 U.S.C. Sec. 254	**Minor** - for purposes of compliance with the Children's Internet Protection Act (CIPA), an individual who has not yet attained the age of seventeen (17). For other purposes, **minor** shall mean the age of minority as defined in the relevant law.

18 U.S.C. Sec. 1460 20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254	**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.
18 Pa. C.S.A. Sec. 5903 18 U.S.C. Sec. 2246	**Sexual Act and Sexual Contact** - as defined at 18 U.S.C. §2246(2) and at 18 U.S.C. §2246(3), and 18 Pa. C.S.A. §5903.
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. **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 Board establishes that access to the school district's technology resources through school resources is a privilege, not a right, which may be revoked at any time. The district's technology resources are the property of the district. The district provides these resources for educational and operational purposes as stated herein and are not provided as a public access service or to provide a public forum.

	The Superintendent or his/her designee is ultimately responsible for overseeing the district's technology resources. The Superintendent will designate the Director of Technology 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 the 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.
20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254	The Superintendent or his/her designee is directed to implement Internet safety measures to effectively address the following, both through general policy and through the use of filtering technology: 1. Access by minors to inappropriate or harmful content. 2. Safety and security of minors when using electronic mail, chat rooms, and social networking. 3. Prevention of unauthorized access of district technology resources. 4. Prevention of unauthorized disclosure and dissemination of minors' personal information.
4. Delegation of Responsibility	The Director of Technology and/or designee will serve as the coordinator to oversee the school district's technology resources and will work with other regional or state organizations as necessary, to educate users, approve activities, provide leadership for proper training for all users in the use of the district technology resources and the requirements of this policy, establish a system to ensure adequate supervision of the district technology resources, maintain executed user agreements, and interpret and enforce this policy. The Superintendent or designee shall ensure students are educated on network etiquette and other appropriate online behavior.
5. Guidelines Policy 815.1	District Provided Resources: District technology resources may be assigned or allocated to an individual user for his or her use (e.g. individual email accounts, laptop computers, etc.). Despite being allocated to a particular user, the technology resources remain the property of the district and may be revoked, suspended, or inspected at any time to ensure compliance with this and other district policies. Users do not have an expectation of

privacy in any district provided technology resource or any of its contents. See Policy 815.1

Monitoring:

District technology resources shall be periodically monitored to ensure compliance with this and other district policies including monitoring of users' online activities. The Director of Technology and/or designee shall ensure that regular monitoring is completed pursuant to this section.

However, in the event of a device being lost or stolen, the Director of Technology and/or designee, may implement procedures to locate that lost or stolen district technology resource through tracking software. Tracking software will not be utilized to track the whereabouts or movements of individuals. In addition, the district will not remotely activate cameras and/or microphones.

Security:

System security is protected through the use of passwords and encryption. 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.

School District Limitation **of** Liability

The district will educate staff and students on best practices and will assist in the event of a data loss or service interruption, but ultimately the district is not responsible, and will not be held responsible, for any loss of data and or documents, any delays, nondelivered and or missed deliveries of electronic communications, or services interrupted. Staff and students may use the district's technology resources at their own risk.

Prohibitions

The use of the school district's technology resources for illegal, inappropriate, unacceptable, or unethical purposes by users is prohibited. Such activities engaged in by users are strictly prohibited and illustrated below. The school district reserves the right to determine if any activity not appearing in the list below constitutes an acceptable or unacceptable use of the district technology resources.

General Prohibitions –

1. Use of technology resources to violate the law, facilitate illegal activity, or to encourage others 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, 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 users' 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. Without permission or authorization of the user or the district, 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, unauthorized interference, unauthorized possession, or unauthorized distribution of confidential or private information. An example includes a user accessing another student's grades and or schedule.

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 on school district technology resources that are 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. Political Lobbying, as defined by the Pennsylvania Lobbying Registration, as amended, and the Pennsylvania Election Code, as amended. District employees and students may use the system to communicate with their elected representatives and to express their opinion on political issues.

21. 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.

22. The use of proxies or other means to bypass Internet content filters and monitoring.

23. The use of technology resources to gamble.

24. Unauthorized access into a restricted system or changing settings or access rights to a restricted system or account.

25. The use of encryption software that has not been previously approved by the district.

26. Sending unsolicited mass email messages, also known as spam.

27. Scanning the district's technology resources for security vulnerabilities.

Access and Security Prohibitions –

Users must immediately notify the Director of Technology and/or designee if they have identified a possible security problem.. The following activities related to access to the school district's technology resources and information are prohibited:

1. Misrepresentation (including forgery) of the identity of a sender or source of communication.

2. Acquiring or attempting to acquire passwords of another user. Users will be held responsible for any misuse of their username or passwords, resulting from sharing their password, leaving passwords unprotected or devices left unattended and accessible, whether intentional or through negligence.

3. Using or attempting to use computer accounts of others; these actions are illegal, even with consent, or if only for the purpose of "browsing".

4. Altering a communication originally received from another person or computer with the intent to deceive.

5. Using school district resources to engage in any illegal act, which may threaten the health, safety or welfare of any person or persons, such as arranging for a drug sale or the purchase of alcohol, engaging in criminal activity, or being involved in a terroristic threat against any person or property.

6. Disabling or circumventing any school district security, program or device, for example, but not limited to, anti-spyware, anti-spam software, and virus protection software or procedures.

7. Transmitting electronic communications anonymously or under an alias unless authorized by the school district.

Operational Prohibitions –

The following operational activities and behaviors are prohibited:

1. Interference with or disruption of the district technology resources, network accounts, services or equipment of others, including, but not limited to, the propagation of computer worms and viruses, Trojan Horse and trapdoor program code, distasteful jokes, and the inappropriate sending of broadcast messages to large numbers of individuals or hosts. The user may not hack or crack the network or others' computers, whether by parasiteware or spyware designed to

steal information, or viruses and worms or other hardware or software designed to damage the district technology resources, or any component of the network, or strip or harvest information, or completely take over a person's computer, or to "look around".

2. Altering or attempting to alter files, system security software or the systems without authorization.

3. Unauthorized scanning of the district technology resources for security vulnerabilities.

4. Attempting to alter any school district computing or networking components (including, but not limited to, fileservers, bridges, routers, or hubs) without authorization or beyond one's level of authorization.

5. Unauthorized wiring, including attempts to create unauthorized network connections, or any unauthorized extension or re-transmission of any computer, electronic communications systems, or network services, whether wired, wireless, cable, or by other means.

6. Connecting unauthorized hardware and devices to **the district technology resources.**

7. Loading, downloading, or use of unauthorized games, programs, files, or other electronic media, including, but not limited to, downloading music files.

8. Intentionally damaging or destroying the integrity of the school district's electronic information.

9. Intentionally destroying the school district's computer hardware or software.

10. Intentionally disrupting the use of the district technology resources.

11. Damaging the school district's technology resources or networking equipment through the users' negligence or deliberate act.

12. Failing to comply with requests from appropriate teachers or school district administrators to discontinue activities that threaten the operation or integrity of the district technology resources.

	Content Guidelines Information electronically published on the school district's technology resources shall be subject to the following guidelines: 1. Published documents including, but not limited to, audio and video clips or conferences, may not include a student's phone number, street address, or box number, name (other than first name) or the names of other family members without parental consent. 2. Documents, web pages, electronic communications, or videoconferences may not include personally identifiable information that indicates the physical location of a student at a given time without parental consent. 3. Documents, web pages, electronic communications, or videoconferences may not contain objectionable materials or point directly or indirectly to objectionable materials.
Pol. 814	4. Documents, web pages and electronic communications must conform to all school district policies and guidelines, including the copyright policy. 5. Documents to be published on the Internet must be edited and approved according to school district procedures before publication. Due Process The school district will cooperate with the school district's Internet Service Provider (ISP) rules, local, state, or federal officials to the extent legally required in investigations concerning or relating to any illegal activities conducted through the school district's technology resources. If students or employees possess due process rights for discipline resulting from the violation of this policy, they will be provided such rights. The school district may terminate the account privileges by providing notice to the user. Search and Seizure User violations of the district's Acceptable Use Policy, the Student Disciplinary Code, district policy or the law may be discovered by routine maintenance and monitoring of the district system, or any method stated in this policy, or pursuant to any legal means. Users' violations of this policy, any other school district policy, or the law may be discovered by routine maintenance and monitoring of the school district system or any method stated in this policy, or pursuant to any legal means.

	District employees should be aware that their personal files may be discoverable and could be discoverable in the event of any form of litigation. Everything that district employees place in their personal files should be written as if a third party would review it. The school district reserves the right to monitor, track, log and access any electronic communications, including, but not limited to, Internet access and emails at any time, for any reason. Users should not have the expectation of privacy in their use of the school district's CIS systems, and other school district technology, even if they misuse the CIS system for personal reasons. Further, the school district reserves the right, but not the obligation, to legally access any personal technology device of students and employees brought onto the school district's property or at school district events, or connected to the school district network, containing school district programs or school district or student data (including images, files, and other information) to ensure compliance with this policy and other school district policies, to protect the school district's resources, or to obtain information/data that the school district reasonably believes involves criminal activity. The district reserves the right to monitor any electronic communications, including but not limited to Internet access and emails. Students and employees should not have the expectation of privacy in electronic communications, even when used for personal reasons. Everything that users place in their personal files should be written as if a third party will review it. <u>Copyright Infringement and Plagiarism</u>
17 U.S.C. Sec. 101 et seq Pol. 814	Federal laws, cases and guidelines pertaining to copyright will govern the use of material accessed through the school district resources. Users will make a standard practice of requesting permission from the holder of the work and complying with license agreements. Employees will instruct users to respect copyrights, request permission when appropriate, and comply with license agreements. Employees will respect and comply as well. Violations of copyright law can be a felony and the law allows a court to hold individuals personally responsible for infringing the law. The school district does not permit illegal acts pertaining to the copyright law. Therefore, any user violating the copyright law does so at their own risk and assumes all liability. Violations of copyright law include, but are not limited to, the making of unauthorized copies of any copyrighted material (such as commercial software, text, graphic images, audio and video recording), distributing copyrighted materials over computer networks, deep-linking and framing into the content of others' websites. Further, the illegal installation of copyrighted software or files for use on the district's computers is expressly prohibited. This includes all forms of licensed software – shrink-wrap, clickwrap and electronic software downloaded from the

	Internet.
Pol. 243	School district guidelines on plagiarism will govern use of material accessed through the school district's technology resources. Users will not plagiarize works that they find. Teachers will instruct students in appropriate research and citation practices. <u>Selection **of** Material</u> School district policies on the selection of materials will govern use of the school district's technology resources. When using the Internet for class activities, teachers will select material that is appropriate for students and that is relevant to the course objectives. Teachers will preview the materials and websites they require or recommend students access to determine the appropriateness of the material contained on or accessed through the website. Teachers will provide guidelines and lists of resources to assist their students in channeling their research activities effectively and properly. Teachers will assist their students in developing the critical thinking skills necessary to ascertain the truthfulness of information, distinguish fact from opinion, and engage in discussions about controversial issues while demonstrating tolerance and respect for those who hold divergent views. Conduct otherwise will result in actions further described in Consequences For Inappropriate, Unauthorized And Illegal Use of this policy and provided in relevant school district policies. <u>Safety **and** Privacy</u> To the extent legally required, users of the school district's technology resources will be protected from harassment or commercially unsolicited electronic communication. Any user who receives threatening or unwelcome communications must immediately send or take them to the Director of Technology and/or designee. Unless part of job function or with authorization by the district, the user may not disclose, use or disseminate personal information of other students or employees including, but not limited to, student's grades, Social Security numbers, home addresses, telephone numbers, school addresses, work addresses, credit card numbers, health and financial information, evaluations, psychological reports, and educational records. Personal contact information includes home address, telephone numbers, school address, and work address.

	Consequences For Inappropriate, Unauthorized And Illegal Use General rules for behavior, ethics, and communications apply when using the district technology 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 of the district technology resources, may result in loss of 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 and professional employee discipline policies, copyright policy, property policies, curriculum policies, terroristic threat policy and harassment policies.
24 P.S. Sec. 4604	The user is responsible for damages to the network, equipment, electronic communications systems, and software resulting from deliberate and willful acts. The user will also be responsible for incidental or unintended damage resulting from willful or deliberate violations of this policy. Violations as described in this policy may be reported to the school district, appropriate legal authorities, whether the ISP, local, state, or federal law enforcement. The school district will cooperate to the extent legally required with authorities in all such investigations. Vandalism will result in cancellation of access to the school district's technology resources and resources and is subject to discipline. References: School Code – 24 P.S. Sec. 1303.1-A, 1317.1 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

	Children's Internet Protection Act Certifications, Title 47, Code of Federal Regulations – 47 CFR Sec. 54.520 Board Policy – 103, 218, 218.2, 220, 233, 237, 243, 248, 249, 317, 348, 814