SUSQUEHANNA TOWNSHIP SCHOOL DISTRICT

SECTION: OPERATIONS

TITLE: ACCEPTABLE USE OF ELECTRONIC RESOURCES

ADOPTED: January 23, 2017

REVISED:

815. ACCEPTABLE USE OF ELECTRONIC RESOURCES

1. Purpose

The Susquehanna Township School District provides its 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 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 enjoy access to the District's technology resources and that such resources are utilized in an appropriate manner and for legitimate purposes.

2. Authority

The Board establishes that access to and use of its technology 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 designee is ultimately responsible for overseeing the District's technology resources. The Superintendent or designee 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 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. The Superintendent or designee is directed to implement Internet safety measures to effectively address the following, both through general policy, procedures 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. 5. Makes every effort to ensure that this resource is used responsibly by students and staff. 6. Inform staff, students, parents/guardians and other users about this policy through any appropriate methods.
Children's Internet Protection Act 47 U.S.C. § 254 34 C.F.R. 54.520	7. Prior to being given access or being issued equipment, inform staff, students, parents/guardian and other users that the district may use monitoring systems to monitor and detect inappropriate use and tracking systems to track and recover lost or stolen equipment.
Child Internet Protection Act 24 P.S. § 4601 et seq.	8. The district shall adhere to the requirements of the Children's Online Privacy Protection Act and shall obtain written parental permission to create accounts for children under the age of thirteen (13).
3. Definition	**District Technology Resources** 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.

4. Guidelines Pol. 218, 815, 249	**User** 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. <u>Un-authorized 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. Further, the District may decrypt any communications or internet traffic to ensure adherence to this policy. <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 e-mails and messages, as well as any files stored on District technology resources may be inspected at any time for any reason. <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 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 pursuant to the established procedure.

Although Susquehanna Township School District uses filtering software, all parties must be aware that filters are imperfect. Material that should not get through sometimes does get through and material that should not be blocked at times does get blocked.

The Board directs that the Superintendent or 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.

Monitoring

District technology resources shall be periodically monitored to ensure compliance with this and other District policies including monitoring of users' online activities. The network administrator designated by the Superintendent shall ensure that regular monitoring is completed pursuant to this section. District technology resources are not to be utilized to track the whereabouts or movements of individuals, and remotely activated cameras and/or audio are not to be utilized. Exceptions to this section may be authorized in advance of such action by the Superintendent or designee to ensure compliance with District policies.

District Provided Resources

District technology resources may be assigned or allocated to an individual user for his or her use. 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.

Safety

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; students to a teacher or administrator and staff to an administrator.

Students are to be reminded to follow safe Internet communications practices as outlined below:

- Never meet anyone in person whom you have met online.

- Remember never to write any personal things about yourself in your online profile.

	• Be civil and polite online. • If people are conducting themselves poorly online, leave and report the conduct to a teacher. • Report any activity that makes you uncomfortable or if someone sends you inappropriate e-mail. • Remember that you need to know who the other person is online. • Do not do things online that you know you wouldn't do in real life. • If you find an inappropriate website, just click the back button and go somewhere else, then report the incident to a teacher or administrator. <u>Security</u> 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. Users are not to allow any other person to use their password or share their account. Teachers and other staff shall not allow students to use their accounts. 4. Any user identified as a security risk or having a history of problems with other computer systems may be limited or denied access to the network. 5. Administration reserves the right to access any user's account in the event of suspected violations of policy. <u>Consequences for Inappropriate Use of District Technology</u> 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 policy and/or local, state, and/or federal law.
5. Delegation of	The Superintendent or designee shall develop procedures, in cooperation with the

Responsibility	District technology staff, for the acceptable use of all District technology resources including, but not limited to: software, hardware, electronic devices, servers, and networks. Such procedures shall be attached to this policy.
6. Limitation of Liability	The District makes no warranties and makes no endorsement of any kind, whether express or implied, for the service it is providing through its various technology resources. The District is not responsible, and will not be responsible, for any damages, including loss of data resulting from delays, non-deliveries, missed deliveries, or services interruption. Use of any information obtained through the District's technology resources is at the user's own risk. The district shall not be responsible for any unauthorized charges or fees resulting from access to the Internet or other network resources. References: Children's Internet Protection Act - 47 U.S.C. § 254 34 C.F.R. 54.520 School Code – 24 P.S. § 4601 et seq Board Policy – 218, 815, 249