No. 815

SECTION: OPERATIONS

TITLE: ACCEPTABLE USE OF THE COMPUTERS, NETWORK, INTERNET, ELECTRONIC COMMUNICATIONS AND INFORMATION SYSTEMS

EAST STROUDSBURG AREA SCHOOL DISTRICT

ADOPTED: April 19, 2002

REVISED: August 18, 2003
April 19, 2004
December 17, 2007
September 15, 2008
April 19, 2010
July 18, 2011
September 17, 2018

815. ACCEPTABLE USE OF THE COMPUTERS, NETWORK, INTERNET, ELECTRONIC COMMUNICATIONS AND INFORMATION (CIS) SYSTEMS[1]

TABLE OF CONTENTS

1. Purpose
2. Definitions
3. Authority
4. Responsibility
5. Delegation of Responsibility
6. Guidelines
   - Access to the CIS Systems
   - Parental Notification and Responsibility
   - School District Limitation of Liability
   - Facsimile Machine and Services
   - Student Use of Electronic Communications Devices (ECDs)
   - Drones
   - 3D Printers
   - Wearable Technology
   - Prohibitions
   - Copyright Infringement and Plagiarism
   - School District Website and Social Media Posting
   - Blogging
   - Safety and Privacy
   - Cloud, Virtual and Online Storage of School District Information and Data
   - Consequences for Inappropriate, Unauthorized, and Illegal Use

1. Purpose

[1]See Definition section for the defined terms generally provided in initial capital letters throughout this Policy and the accompanying Administrative Regulation.

1.1 The East Stroudsburg Area School District ("School District") provides employees, students, and registered Guests ("Users") with School District resources, including, computers, hardware, software, and access to the School District's Electronic Communication System, networks, which includes internet access, whether wired, wireless, cellular, virtual, cloud, or by any other means, and electronic information sources, as detailed below. Guests include, but are not limited to, visitors, workshop attendees, volunteers, adult education staff, students, School Board members, independent contractors, vendors, and School District consultants.

1.2 School District Computers, ECDs, networks, internet, Intranet, Electronic Communications Systems and services, information and data systems and services, databases, files, software, and media, collectively called "CIS Systems," provide vast, diverse and unique resources. The Board of School Directors will make available access to the School District's CIS Systems for Users if there is a specific School District-related purpose: for example, to access information, to research; to facilitate learning and teaching; to support School District business; and/or to foster the Educational Purpose and mission of the School District.

1.3 For Users, the School District's CIS Systems must be used for Educational Purposes and/or performance of School District job duties in compliance with this Policy and accompanying Administrative Regulation #815, other School District policies, regulations, rules, and procedures; internet service provider's ***(ISP)*** websites' and apps' terms (if they are lawful), and local, state, and federal laws and procedures ***(School District Policies and Other Legal Requirements)***. ***Incidental Personal Use*** of the School District's CIS Systems is permitted for employees as defined in this Policy. Students may only use the CIS systems for Educational Purposes.

1.4 All Users should have no expectation of privacy in anything they create, store, send, receive, or display on or over the School District's hardware, software and CIS Systems, including their personal files, or any of their use. For example, when *Users bring and use their own personal Computers, personal electronic communication devices **(PECDs)**, or other entities Computers or ECDs, or use the School District's electronic communication devices **(SD ECDs)*** that are located or installed on School District property, at School District events, connected to the School District's network and/or systems, or when using its mobile computing equipment, telecommunication facilities in unprotected and protected areas or environments, directly from home, or indirectly through another ISP.

1.5 If Users bring personal Computers or PECDs onto the School District's property, to School District events, or connect them to the School District's

	network and systems, and if the School District reasonably believes the personal Computers and PECDs contain School District information or contain information that violates a School District Policy and/or Other Legal Requirements, the legal rights of the School District or another person, or involves significant harm to the School District or another person, or involves a criminal activity, the personal Computers or PECDs may be *legally accessed in accordance with the law* to insure compliance with this Policy, and/or Other Legal Requirements Users may not use their personal Computers and PECDs to access the School District's intranet, internet or CIS Systems unless approved by the Director of Technology, and/or designee. 1.6 The School District intends to strictly protect its CIS Systems against numerous harms, including 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 accompanying administrative regulation, and to immediately report any violations or suspicious activities to the Superintendent, and/or designee. Noncompliance will result in actions further described in the "Consequences for Inappropriate, Unauthorized and Illegal Use" section found in the last section of this Policy, and provided in other relevant School District Policies and Other Legal Requirements. 1.7 This is a comprehensive Policy that addresses the School District's acceptable use of its communication, technology, and information systems. It also refers to and incorporates other technology-related School District's policies. All of these policies may be modified as the electronic and digital information environment evolves.
2. Definitions	**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; 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. §6312(d); 24 P.S. § 4603	Under Pennsylvania law, any person who intentionally views or knowingly possesses or controls 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 is guilty of a felony of the third degree for their first offense, or is guilty of a felony of the second degree for a second offense.
20 U.S.C. § 6777 (e); 18 U.S.C. § 2256(6) Policy 237	**Computer**– 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 information and/or data (including images, files, and/or texts) attached or connected to, installed in, or otherwise used in connection with a Computer. For example, *Computer* includes, but is not limited to, the School District's and Users': • Desktop, notebook, powerbook, tablet PC or laptop computers; • Servers, firewalls/security systems, distance learning equipment, videoconference units, printers, facsimile machine, cables, and other peripherals; • Specialized electronic equipment used for students' special educational purposes; • RFID, and Global Positioning System ***(GPS)*** equipment; • Personal digital assistants ***(PDAs)***; • iPads, iPods, MP3 players, and electronic readers; • USB/jump drives; • iPhones, cell phones, with or without internet access, and/or recording, electronic mail, camera/video, and/or other capabilities and configurations, telephones, mobile phones, or wireless devices, two-way radios/telephones and other smartphones; • Beepers,; paging devices, laser pointers and attachments; • Internet of Things items (everyday objects that have network connectivity, allowing them to send and receive data), including vehicles with smart technology, and wearable smart devices that can be worn by a person, either as an accessory or as part of material used in the clothing, and is able to be connected to the Internet enabling data to be exchanged between a network and the device (for example, smart watches, smart clothing, fitness trackers, football helmets, and smart jewelry); • Virtual reality and augmented reality headsets, helmets and services; • Computerized drones, and any other such technology developed.

Electronic Communication Devices ("ECDs") – *ECDs* are communication devices with voice, data, text, and/or navigation capabilities that are able to access the internet, transmit telephone calls, text messages, email messages, instant messages, video communications (such as iChat and Skype), perform word processing and other Computer and online applications (apps), and provide location information. The devices are capable of electronically communicating, sending, receiving, storing, recording, reproducing, and/or displaying information and data.

Examples of ECDs include, cellular phones, smartphones (iPhone), mobile phones (with email, recording and/or camera/video and other capabilities and configurations); traditional telephones; pagers/beepers; location tracking devices, GPS instruments; Computers; portable game units; graphic calculators; MP3, music, and media players; PDAs; digital cameras; tablets (such as iPads and e-Readers) and laptop Computers; wearable technology; drones; and other devices that can capture still images or video, can record, store, display, transmit, or receive audio and/or video with digital, electronic, wired, wireless, or cellular communication capabilities. ECDs may also be referred to as electronic devices in other publications and School District policies.

ECDs could be devices that are not capable of transmitting telephone communications (such as radios), do not have internet access, are lasers, and/or are radar communication devices.

ECDs could be issued to students or employees by the School District (SD ECDs), or ECDs could be owned by the students or employees (PECDs).

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, photooptical or photoelectronic facilities for the transmission/transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature, of wire or electronic communications, and any Computer facilities or related electronic equipment for the electronic storage of such communications.

Examples include, without limitation, the internet, intranet, voice mail services, electronic mail services, tweeting, text messaging, and social media.

Educational Purpose - Includes use of the CIS systems for classroom activities, professional or career development, and to support the School District's curriculum,

	policies, regulations, rules, procedures, and mission statement.
20 U.S.C. § 6777(e)(6);	**Harmful to Minors**- Under Federal law, any picture, image, graphic image file or other Visual Depictions that:
47 U.S.C. § 254(h)(7) (G)	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, and 3. Taken as a whole lacks serious literary, artistic, political, educational or scientific value as to Minors.
18 Pa.C.S.A. § 5903 (e)(6); 24 P.S. § 4603	Under Pennsylvania law, that quality of 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; and, 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. **Inappropriate Matter** - Includes, but is not limited to visual, graphic, video, text and any other form of indecent, Obscene, pornographic, sexually explicit, Child Pornographic, dangerous, unsafe or other material that is Harmful to Minors Examples include, taking, disseminating, transferring, or sharing Obscene, pornographic, lewd, or otherwise illegal images or photographs, whether by electronic data transfer or otherwise (such as sexting, e-mailing, texting, among others). Others include, hateful, illegal, defamatory, lewd, vulgar, profane, inflammatory, threatening, harassing, discriminatory (as it pertains to race, color, religion, national origin, gender, marital status, age, sexual orientation, political beliefs, receipt of financial aid, or disability), violent, bullying/cyberbullying, sexting, flagging, terroristic unlawful, and/or, obscene 3D objects that are unsafe, harmful, dangerous, or pose a threat to the well-being of the User or to others, as well as other Inappropriate Matter and material specified, throughout this Policy, and other School District Policies and Other Legal Requirements. It also includes

	advocating the destruction of property. **Incidental personal use** - *Incidental Personal Use* of school Computers and CIS Systems are permitted for employees so long as such use does not interfere with the employee's job duties and performance, with system operations, or with other system Users. Personal use must comply with School District Policies, its accompanying administrative regulation, and Other Legal Requirements, and must not damage the School District's hardware, software, and CIS Systems.
20 U.S.C. § 6777 (e); 47 U.S.C. § 254 (h)(7)(D); 18 U.S.C. § 2256; 18 Pa.C.S.A. § 5903(e)	**Minor**- For purposes of compliance with the Federal Children's Internet Protection Act ("FedCIPA"), 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. § 1460; 20 U.S.C. § 6777(e; 47 U.S.C. § 254(h)(7)(E)	**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; and 3. Whether the work taken as a whole lacks serious literary, artistic, political, educational, or scientific value.
18 Pa.C.S.A. § 5903(b); 24 P.S. § 4603	Under Pennsylvania law, 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.

18 U.S.C. § 2246; 18 Pa.C.S.A. § 5903 (e)(3); 20 U.S.C. § 6777(e); 47 U.S.C. § 254(h)(7)(H)	**Sexual Act and Sexual Contact**- As defined at 18 U.S.C. § 2246(2), at 18 U.S.C. § 2246(3), and at 18 Pa. C.S.A. § 5903.
47 U.S.C. § 254(h)(7)(I); 24 P.S. § 4606	**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.
18 Pa.C.S.A. § 2256 18 Pa. C.S.A. § 6321	**Visual Depictions**– Under Federal law - Includes undeveloped film and videotape, data stored on a Computer disk or by electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format. Under Pennsylvania law – A representation by picture, including, but not limited to, a photograph, video tape, film, or computer image.
3. Authority 47 U.S.C. § 254(l); 24 P.S. § 510; 24 P.S. § 4604	3.1 Access to the School District's CIS Systems through school resources is a privilege, not a right. These CIS Systems and Resources, as well as the User accounts and information, are the property of the School District. The School District further reserves the right to deny access to prevent unauthorized, inappropriate or illegal activity, and may revoke those privileges and/or administer appropriate disciplinary action. The School District will be reasonably cooperative with other educational entities, ISPs, websites, and appropriate authorities, and local, state, and federal officials to the extent legally required in any investigation and will follow process and/or procedure concerning or related to the misuse of the CIS systems, whether criminal or civil actions. 3.2 It is often necessary to access Users' accounts in order to perform routine maintenance and security tasks. System administrators have the right to access by interception, and to access the stored communication of Users' accounts for any reason in order to uphold School District Policies and Other Legal Requirements, and to maintain the systems. **3.3 USERS SHOULD HAVE NO EXPECTATION OF PRIVACY IN ANYTHING THEY CREATE, STORE, SEND, RECEIVE, OR DISPLAY ON OR OVER THE SCHOOL DISTRICT'S CIS SYSTEMS, AND THE SCHOOL DISTRICT'S AUTHORIZED THIRD PARTIES SYSTEMS, INCLUDING THEIR PERSONAL FILES OR ANY OF THEIR USE OF THESE CIS SYSTEMS.**

	The School District reserves the right to access, view, record, check, receive, monitor, track, log, store, and otherwise inspect and utilize any or all School District CIS Systems', and authorized third parties' systems, and to monitor and allocate fileserver space. Users of the School District's CIS systems, and authorized third parties' systems, who transmit or receive communications and information shall be deemed to have consented to having the content of any such communications accessed, viewed, recorded, checked, received, monitored, tracked, logged, stored, and otherwise inspected or used by the School District, and to the School District monitoring and allocating fileserver space. Passwords and message delete functions do not restrict the School District's ability or right to access such communications or information.
20 U.S.C. § 6777(c); 24 P.S. § 4610 47 U.S.C. § 254	3.4 The School District reserves the right to restrict access to any internet sites or functions it may deem inappropriate through general policy, software blocking or online server blocking. Specifically, the School District operates and enforces Technology Protection Measure(s) that block or filter online activities of Minors, where possible, on its Computers used and accessible to adults and students so as to filter or block Inappropriate Matter. The Technology Protection Measure must be enforced during use of Computers with internet access. Measures designed to restrict adults' and Minors' access to material Harmful to Minors may be disabled to enable an adult or a student (who has provided written consent from a parent or guardian) to access *bonafide* research, not within the prohibitions of this Policy, its accompanying administrative regulation, or for another lawful purpose. No person may have access to material that is illegal under federal, state, or local law.
20 U.S.C. § 6777(c); 24 P.S. § 4610	3.5 Expedited review and resolution of a claim that the Policy and/or its administrative regulation is denying a student or adult to access material will be enforced by an administrator, supervisor, or their designee, upon the receipt of written consent from a parent or guardian for a student, and upon the written request from an adult presented to the Director of Information Technology and/or Assistant Superintendent for Curriculum and Instruction.
	3.6 The School District has the right, but not the duty, to inspect, review, or retain electronic communications created, sent, displayed, received or stored on and over its CIS Systems; to monitor (electronic or otherwise), record, check, track, log, access or otherwise inspect; and/or to report all aspects of its CIS systems use. This includes any *User's personal Computers*, *PECDs*, networks, internet, Electronic Communication Systems, Computers, databases, files, software, and media that they bring onto School District property, or to School District events, that are connected to the School District systems and/or network, or when using

the School District's mobile commuting equipment, telecommunications facilities in protected and/or unprotected areas or environments, directly from home, or indirectly through another ISP, and if relevant, *when Users bring and use another entity's Computer or ECD* to School District location, event, or connect it to a School District networks and/or systems, and/or that contain School District programs, or School District or Users' data or information, all pursuant to the law, in order to insure compliance with this Policy, its administrative regulation, and other School District Policies and Other Legal Requirements, to protect the School District's resources, and to comply with the law.

3.7 The School District reserves the right to restrict or limit usage of lower priority CIS Systems, Computers, PECDs, SD ECDs, and ECDs use when network and computing requirements exceed available capacity according to the following priorities:

3.7.1. Highest- uses that directly support the education of the students, and the business operations of the School District.

3.7.2. Medium- uses that indirectly benefit the education of the student, and the business operations of the School District.

3.7.3. Lowest- uses that include reasonable and limited educationally-related employee interpersonal communications and employee limited Incidental Personal Use.

3.7.4. Forbidden- all activities in violation of the School District Policies and Other Legal Requirements.

3.8 The School District additionally reserves the right to:

3.8.1. Determine which CIS Systems' services will be provided through School District resources.

3.8.2. Determine the types of files that may be stored on School District file servers and Computers and SD ECDs.

3.8.3. View and monitor network traffic, fileserver space, processor, and system utilization, and all applications provided through the network and Electronic Communications Systems, Computers and ECDs.

3.8.4. Remove excess e-mail and other electronic communications or files taking up an inordinate amount of fileserver space after a reasonable time.

	3.8.5. Revoke User privileges, remove User accounts, or refer violations to legal authorities, and/or School District authorities when violation of this and any other applicable School District Policies and Other Legal Requirements are violated, including, but not limited to, those governing network use, copyright, security, privacy, employment, social media, vendor access, data breach, and destruction of School District resources and equipment.
Previous ESASD Policy #717	3.9 The Board authorizes the purchase and use of School District cellular telephones and ECDs for employees, if determined to be necessary by the Superintendent, and/or designee. Cellular telephones and SD ECDs provided to employees shall be used for authorized School District business purposes. Personal use is prohibited, unless use has been approved by the Superintendent, and/or designee.
4. Responsibility	4.1. The Superintendent is granted the authority to create, modify, update, and enforce an administrative regulation to accompany this Policy. The administrative regulation must include, among other sections: Prohibitions (*General Prohibitions, Access and Security Prohibitions,* and *Operational Prohibitions),* Content Guidelines, Due Process, Search and Seizure, and Selection of Material. This Policy must be incorporated into the administrative regulation. 4.2. Due to the nature of the internet, Inappropriate Matter can be accessed through the CIS Systems and Electronic Communications Systems. Because of the nature of the technology that allows the internet to operate, the School District cannot completely block or filter access to these resources. Accessing these and similar types of resources may be considered an unacceptable use of School District resources and will result in actions explained further in the Consequences for Inappropriate, Unauthorized and Illegal Use section found in the last section of this Policy, its accompanying administrative regulation, and as provided in other relevant School District Policies and Other Legal Requirements. 4.3. The School District must publish a current version of this Policy and its accompanying administrative regulation so that all Users are informed of their responsibilities. A copy of this Policy, its accompanying administrative regulation, and *CIS Acknowledgement and Consent Form(s)* must be provided to all Users, who must sign the School District's *CIS Acknowledgement and Consent Form(s),* either by electronic or written means. 4.4. Employees must be proficient in, capable of, and able to use the School District's CIS Systems, and software relevant to the employee's responsibilities. In addition, Users must practice proper etiquette, School District ethics, and agree to the requirements of School District Policy and Other Legal

	Requirements.
5. <u>Delegation of Responsibility</u>	5.1. The Director of Technology, and/or designee, will serve as the coordinator to oversee the School District's CIS Systems 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 CIS Systems and the requirements of this Policy, its accompanying administrative regulation, establish a system to insure adequate supervision of the CIS Systems, maintain executed User *CIS Acknowledgement and Consent Forms*, and interpret and enforce Policy and its accompanying administrative regulation.
Policy 800 & 800AR	5.2. The Director of Technology, and/or designee, must establish a process to set up individual and class accounts, to set quotas for disk usage on the system, establish a Record Retention and Records Destruction Policy and Records Retention and Destruction Schedule to include electronically stored information (see School District Policy #800), and establish the School District malware and security protection process.
	5.3. Unless otherwise denied for cause, student access to the CIS Systems resources must be through supervision by the professional staff. Administrators, teachers and staff have the responsibility to work together to help students develop the skills and judgment required to make effective and appropriate use of the resources. All Users have the responsibility to respect the rights of all other Users within the School District, to protect and use the School District CIS Systems wisely, and to abide by the School District's Policies and Other Legal Requirements.
47 U.S.C. § 254 (5)(B)(iii); 24 P.S. § 1303.1-A; Policy 249	5.4 The Assistant Superintendent for Curriculum and Instruction, and/or designee, has the responsibility to educate Minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.
6. Guidelines	6.1. <u>Access to The CIS Systems</u>
	6.1.1 The CIS Systems accounts of Users must be used only by authorized Users/owners of the accounts and only for authorized purposes.
	6.1.2 An account must be made available according to a procedure developed by appropriate School District authorities if an individual meets the requirements to be granted an account. The School District may deny or refuse to grant account.
	6.1.3 CIS System. This Policy, its accompanying administrative regulation, as well as Other School District Policies and Other Legal Requirements, will

govern use of the hardware, software, information, and School District's CIS Systems for Users.

6.1.4 Types of Services include, but are not limited to:

(1) Internet - School District employees, students, and Guests will have access to Internet through the School District's CIS Systems, as needed.

(2) E-Mail, Text Messaging, and Skype - School District employees may be assigned individual e-mail text messaging, and Skype accounts for work-related use, as needed. Students may be assigned individual e-mail accounts, as necessary, by the Director of Technology, and/or designee, at the recommendation of the teacher who will also supervise the students' use of the e-mail service. Parents of students in the East Stroudsburg Area School District Virtual Academy must also supervise the child in his/her use of the School District's e-mail service. Students and Guests may not be assigned text message and Skype accounts.

(3) Guest Accounts –Registered Guests may receive an individual internet account with the approval of the Director of Technology, and/or designee, if there is a specific School District-related purpose requiring such access. Use of the CIS Systems by a Guest must be specifically limited to the School District-related purpose and comply with this Policy, its accompanying administrative regulation, and Other School District Policies and Other Legal Requirements. Guests must not damage the School District's CIS Systems. A School District *CIS Acknowledgment and Consent Form* must be signed, in writing or electronically, by a Guest, and if the Guest is a Minor, a parent's or guardian's written or electronic signature is required.

(4) Blogs - Employees may be permitted to have School District-sponsored blogs, after they receive training, and the approval of the Director of Technology, or designee. All bloggers must follow the rules provided in this Policy, its accompanying administrative regulation, and other School District applicable policies (for example, the Social Media Policy and Social Media Administrative Regulations), and Other Legal Requirements.

(5) Web-based Services - Certain School District authorized web-based services, such as blogging, authorized social media sites, wikis, podcasts, RSS feeds, social software, course management systems, and interactive collaboration tools that emphasize online participatory learning (where Users share ideas, comment on one another's project, plan, design, or implement, advance or discuss practices, goals, and ideas together, co-create, collaborate and share) among Users may be permitted by the School District, however, such use must be approved by the Director of Technology, and/or designee,

	followed by training authorized by the School District. Users must comply with School District Policies and Other Legal Requirements during such use.
	6.2. Parental Notification and Responsibility
24 P.S. § 4604	The School District will notify the parents/guardians about the School District's CIS Systems and the School District's policies, regulations, rules, and procedures governing their use. This Policy and its accompanying regulation contain restrictions on accessing Inappropriate Matter. There is a wide range of material available on the internet, some of which may not be fitting with the particular values of the families of the students. It is not practically possible for the School District to monitor and enforce wide range of social values in student use of the Internet. Further, the School District recognizes that parents/guardians bear primary responsibility for transmitting their particular set of family values to their children(ren). The School District will encourage parents/guardians to specify to their children(ren) what material and matter is and is not acceptable for their children to access through the School District's CIS System. Parents/Guardians are responsible for monitoring their children's use of the School District's CIS Systems when they are accessing the systems.
	6.3. School District Limitation of Liability
	The School District makes no warranties of any kind, either expressed or implied, that the functions or the services provided by or through the School District's CIS Systems will be error-free or without defect. The School District does not warrant the effectiveness of internet filtering. The electronic information available to Users does not imply endorsement of the content by the School District. Nor is the School District responsible for the accuracy or quality of the information obtained through or stored on the CIS Systems. The School District will not be responsible for any damage Users may suffer, including but not limited to, information that may be lost, damaged, delayed, misdelivered, or unavailable when using the CIS Systems. The School District will not be responsible for material that is retrieved through the internet, or the consequences that may result from them. The School District will not be responsible for any unauthorized financial obligations, charges or fees resulting from access to the School District's CIS Systems. In no event will the School District be liable to the user for any damages whether direct, indirect, special or consequential, arising out of the use of the CIS Systems.

	6.4 Facsimile Machines and Services 6.4.1. Whether facsimile (fax) services are provided through a separate fax machine or through a Computer, facsimile transmissions, transmittal sheets, and the fax must be handled securely. 6.4.2. Employees are responsible for sending fax transmissions on behalf of the School District. 6.4.3. Transmissions must include receipt information, such as time and place of sending, must be arranged to reach its intended destination, and, must be properly logged and stored. 6.4.4. Transmittal sheets must include the School District's name, and include language that cautions that the fax is intended to be confidential, and for the use of the individual or entity named on the transmittal sheet. 6.5 Student Use of Electronic Communication Devices
Policy #237 24 P.S. §1317.1	6.5.1. Students are prohibited from visually possessing, using and turning on their PECDs and SD ECDs during the school day in School District buildings, on School District property, and while students are attending School District-sponsored activities during regular school hours on School District premises and property (including but not limited to, buses and other vehicles), at School District events, or through connection to the School District's CIS Systems. PECDs and SD ECDs must be turned off upon entering the School District building and remain off until the student leaves the School District building, unless expressed permission has been granted by a teacher, principal, or administrator. 6.5.2. Students are prohibited from using PECDs and SD ECDs with or without internet access and/or recording, and/or camera/video, and other capabilities and configurations to take videos and images of others, transfer them, or place them on websites or social media without the consent of the person(s) in the image, and/or parent(s)/guardians, and/or building principal. 6.5.3. Students who are performing volunteer fire company, ambulance or rescue squad functions, or need a Computer or PECD due to their medical condition, or the medical condition of a member of their family, with notice and the approval of the school administrator they may qualify for an exemption of this prohibition.

	6.5.4. School District students may possess and Silently Use[2] SD ECDs and PECD's when in compliance with Policy #237, School District Policies and Other Legal Requirements, supportive of the educational program of the School District , and permission is granted by a teacher or administrator.
	6.5.5. However, the possession and use of IU ECDs and PECDs by students that are found to be disruptive to the educational process and/or environment can be abusive in ways that negatively affect students, employees, and the School District's mission, in such cases their use is prohibited in accordance with School District Policies and Other Legal Requirements.
	6.5.6. Students must also comply with the School District Policy #237.
	6.6 Drones
	6.6.1. The School District provides the opportunity for students and employees to learn about and use unmanned aircraft systems (also referred to as "drones") for educational use, whether curricular or extracurricular.
FAA Memorandum, May 4, 2016; 49 U.S.C. 140101 note	6.6.2. The Superintendent and/or designee is responsible for coordinating the drone initiative for the School District. Employees who teach students about drones and their use must utilize sound instructional methods, techniques, and practices, and develop lesson plans that assist them as they provide instruction to meet curricular and extracurricular guidelines. Employees who participate in the students' operation of the drones must comply with School District Policies and Other Legal Requirements, including relevant local, state, and federal laws, such as the Federal Aviation Agency ("FAA") drone regulations, advisory circulars, memos, and interpretations. As one example, *de minimus* limited instructor participation in student operation of drones as part of the coursework does not rise to the level of a faculty member conducting an operation outside of the hobby or recreation construct (where an individual is not being compensated).
14 C.F.R. Parts 101 & 107	6.6.3. The FAA has promulgated rules for drones based on why a drone is flown. Two examples include: (1) for educational or recreational use or (2) for commercial use. Examples for educational or recreational use include educational curricular and extracurricular use. Examples of commercial use include providing aerial surveying, or photography services, and flying incidental to a business (e.g., doing roof inspections or real estate photography). The School District will need to assess on a case-by-case basis why the drone is being flown, then comply with the

[2] See Definition section in the Electronic Communication Devices Policy #237.

legal pilot requirements, aircraft requirements, location requirements, and operating rules, among others. Waivers of the rules may be available through an FAA required procedure.

6.6.4. Employees and students must understand the risks with flying drones, including the safety, security, privacy and other risks.

(1) *Safety*. Anyone operating a drone is responsible for flying pursuant to FAA regulations and guidance. As an important example, where is it safe and where is it not safe to fly. Likewise, a few additional examples include: keeping your aircraft within sight; do not fly over stadiums or sporting events without approval; and follow community-based safety guidelines. Consequently, the School District prohibits any pilot from flying their drone over the School District's facilities, such as sporting events and people, unless the pilot submits a request in writing to the Superintendent and/or designee, receives approval from the Superintendent, and submits written verification that the pilot understands and will comply with the terms of the approval and this policy.

(2) *Privacy and Security*. Drones are basically used for imaging and photography, surveillance, inspection, and reconnaissance to gather, collect and store data for analysis and communication. School District drones may contain various surveillance technologies (such as, cameras for photographs and video, and tracking devices). However, the surveillance technology placed on and/or used on the drones must be approved by the Superintendent. School District drones may not be equipped with unlawful items, such as weapons. The School District must protect the privacy and security of the data that it collects when using its drones, and pilots must not trespass onto the School District's and others property and airspace.

6.6.5. The School District will not be liable currently or in the future for individuals' who misuse a drone on or over the School District's or another person's property, or for pilot violations of School District Polices and Other Legal Requirements, including FAA regulations, and criminal and civil violations.

6.6.6. The Superintendent, and/or designee, is authorized to prepare and enforce administrative regulations and/or rules to carry out the use of drones.

6.7 3D Printers

6.7.1. The School District provides students and employees 3D printers and scanners to use when there is a School District instructional reason for their use. Approval by a teacher or administrator is required for the student or employee to operate a 3D printer and scanner. If approved, the person approving such use must then supervise the students' or employees' use. The School District reserves the right to deny any request.

6.7.2. Use of 3D printers and scanners must comply with School District Policies and Other Legal Requirements. For example, no created object: (i) may violate local, state or federal law; (ii) may involve Inappropriate Matter (as defined in this Policy); (iii) may be unsafe, harmful, dangerous, or may pose an immediate threat to the well-being of others (for example, knives, guns, or lethal weapons); and (iv) may violate the intellectual property rights (copyright, patent, trade secret, trademark) of the owner.

6.7.3. Employees must have training in the use of 3D printers and scanners from a School District approved individual, program, or service. The training must include, among other items: protecting the safety, security and privacy relevant to use of 3D printers and scanners; protecting intellectual property rights with respect to designs, procedures, practices, and software "build files;" infringing by replication; and using the objects produced by 3D printers lawfully. Students must be taught how to safely use 3D printers and scanners, how to protect their privacy and others' privacy, how to not violate others' intellectual property rights, and security; and how to lawfully use the 3D printer and scanner and the objects they created.

6.7.4. Employees must develop a lesson plan and use 3D printers and scanners in a productive and effective way to meet curriculum guidelines.

6.7.5. Employees and students must understand the risks associated with 3D printing, including the physical damage or harm when they are transporting and using a 3D printer and scanner, the malfunctions of a 3D printer, or the defects in the objects. The School District will not guarantee the quality or stability or the confidentiality of the designs, or be liable for any object created with the use of the 3D printers or scanners, including harm or injury incurred as a result of the use of the equipment.

6.7.6. The Superintendent, and/or designee, is authorized to prepare and enforce administrative regulations and/or rules to carry out the use of 3D printers and scanners.

6.8 Wearable Technology

6.8.1. The School District recognizes that students and employees may be wearing personal computing devices for personal or efficiency reasons. These wearables are part of the Internet of Things (defined in the Definition Section in this Policy), that include fitness trackers (tracks wearers' fitness patterns), health trackers (monitor wearers' health conditions), ready-reference devices (provides access to the world of online information), and history-recording devices (records the wearers' experiences).

6.8.2. If students or employees are using the School District's WiFi or Internet service, the students or employees have no expectation of privacy in anything they create, store, send, receive, or display on or over the School District's CIS Systems, including their personal files or any of their use of the School District's CIS Systems. The School District reserves the right to record, check, receive, monitor, track, log, access, and otherwise inspect any or all CIS Systems use and to monitor and allocate fileserver space. The School District does not attempt to collect the information on the wearers' devices.

6.8.3. The School District does not require students or employees to wear or use School District wearable technology. Therefore, the School District does not attempt to collect the information and data through School District wearables.

6.8.4. If a student's or an employee's wearable collects personal information from other individuals, the School District is not liable for the student's or employee's collection, use, storage, or other action(s) with respect to the information or data they collect.

6.8.5. The Superintendent, and or designee, is authorized to prepare and enforce administrative regulations and or rules to carry out issues relevant to wearable technology.

6.9. Prohibitions

6.9.1 The use of the School District's CIS Systems for illegal, inappropriate, unacceptable, or unethical purposes by Users is prohibited. Such activities engaged in by Users are strictly prohibited, including but not limited to the

	activities illustrated and in the accompanying administrative regulation #815. The School District reserves the right to determine if any activity not appearing in the lists constitute an acceptable or unacceptable use of the CIS Systems.
Policy 237	6.9.2 The prohibitions are in effect any time School District resources are accessed whether on School District property, through the East Stroudsburg Area School District Virtual Academy, at School District events, while connected to the School District's network, when using mobile commuting equipment, telecommunication facilities in protected and unprotected areas or environments, directly from home, or indirectly through another ISP, website or app, and if relevant, when a User uses their own equipment. Students must also comply with the School District's Electronic Communication Devices Policy, # 237.
17 U.S.C. § 101 et seq.; Policy 814	6.10. <u>Copyright Infringement and Plagiarism</u> 6.10.1 Federal laws, cases, policies, regulations, and guidelines pertaining to copyright will govern the use of material accessed through School District resources. See School District Policy #814. Users will make a standard practice of requesting permission from the holder of the work, and complying with the Fair Use Doctrine, and/or complying with license agreements. Employees will instruct Users to respect copyrights, request permission when appropriate, and to comply with the Fair Use Doctrine and/or with license agreements. Employees will respect and comply as well. 6.10.2 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. 6.10.3 Violations of copyright law include, but are not limited to, making unauthorized copies of any copyrighted material (such as commercial software, text, graphic images, audio and video recording), distributing copyrighted materials over Computer networks, remixing or preparing mash-ups that violate the law, and deep-linking and framing into the content of others' websites. Further, the illegal installation of copyrighted software or files for use on the School District's Computers, SD ECDs, and PECDs is expressly prohibited. This includes all forms of licensed software -- shrink-wrap, clickwrap, browsewrap, and electronic software and apps, downloaded from the internet.

17 U.S.C. § 1202	6.10.4 No one may circumvent a Technology Protection Measure that controls access to a protected work unless they are permitted to do so by law. No one may manufacture, import, offer to the public, or otherwise traffic in any technology, product, service, device, component or part that is produced or marketed to circumvent a Technology Protection Measure to control access to a copyright protected work.
Policy 814	6.10.5 School District guidelines on plagiarism will govern use of material accessed through the School District's CIS Systems. Users must not plagiarize works. Teachers will instruct students about appropriate research and citation practices. Users understand that use of the School District's CIS Systems may involve the School District's use of plagiarism analysis software being applied to their works.
	6.11 <u>School District Website and Social Media Postings</u>
	6.11.1 The School District has established and maintains a website social media presence on Facebook and Twitter. The School District will develop and modify its information on the web pages and social media sites under the direction of the Director of Technology, and/or designee.
	6.11.2 Publishers must comply with the School District's Social Media Policy, its accompanying administrative regulation, and other School District Policies (for example, the School District's Website Development Policy, #815.1), and Other Legal Requirements.
17 U.S.C. § 512 Policy 814	6.11.3 The School District may limit its liability by complying with the Digital Millennium Copyright Act's safe harbor notice and takedown provisions.
	6.12. <u>Blogging</u>
	6.12.1 If a User creates a blog with their own resources and on their own time, the User may not violate the privacy and security rights of employees and students, may not use School District personal and private information/data, images, equipment, resources, and infringed copyrighted material in their blog, and may not disrupt the operations of the School District. See also the School District's Social Media Policy, and its accompanying administrative regulations.
	6.12.2 Contrary conduct will result in actions further described in the "Consequences for Inappropriate, Unauthorized and Illegal Use" section of this Policy, its accompanying administrative regulation, and provided in other relevant School District Policies and Other Legal Requirements.

47 U.S.C. § 254	6.13. Safety and Privacy 6.13.1 To the extent legally required, Users of the School District's CIS Systems will be protected from harassment or commercially unsolicited electronic communication. Any User who receives threatening or unwelcomed communications must immediately send or provide and/or show them to the Director of Technology and/or designee. 6.13.2 Users must not post unauthorized personal contact information about themselves or other people on the CIS Systems. Users may not steal another's identity in any way, may not use spyware, cookies, or other program code, keyloggers, and may not use School District or personal technology or resources in any way to invade another's privacy and security. Additionally, Users may not disclose, use or disseminate confidential and personal information about students or employees, unless legitimately authorized to do so. Examples of prohibited postings include, but are not limited to, revealing: biometric data, student grades, Social Security numbers, dates of birth, home addresses, telephone numbers, school addresses, work addresses, credit card numbers, health and financial information, evaluations, psychological reports, educational records, reports, and resumes or other information relevant to seeking employment at the School. 6.13.3 If the School District requires that data and information to be encrypted. Users must use School District authorized encryption to protect their security. 6.13.4 Users, by their use of the School District's CIS Systems, agree not to meet with someone they have met online unless they have parental consent. 6.14 Cloud, Virtual, and Online Storage of School District Information and Data Users must keep all School District information (including but not limited to employees and students) in the School District's and it's contracted parties' storage, unless permission is granted in writing by the Superintendent, and/or designate. This means that employees, students, and Guests must not place School District information in cloud, virtual, or online storage beyond the control, access, protection, and safety of the School District, unless specific permission is granted in writing by the Superintendent, and/or designee, and the student, employee, and Guest agree to comply with the School District's terms and conditions, including but not limited to safety, security, privacy, location, and the School District's access.

6.15. Consequences for Inappropriate, Unauthorized and Illegal Use

6.15.1 General rules for behavior, ethics, and communications apply when using the School District's hardware, software, CIS Systems and information, in addition to the stipulations of this Policy, and its accompanying administrative regulation, additional School District Policies and Other Legal Requirements. Users must be aware that violations of this Policy, its accompanying Administrative Regulation, or School District Policies and Other Legal Requirements, or for unlawful use of the CIS Systems, 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, student suspensions, employee suspensions (with or without pay), dismissal, expulsions, breach of contract, and/or legal proceedings. This will be handled on a case-by-case basis. This Policy, and its accompanying administrative regulation, incorporate all other relevant School District policies, such as, but not limited to, the student and professional employee discipline policies, Code of Student Conduct, copyright, social media, data breach, security, property, curriculum, terroristic threat, vendor access, student electronic communication devices and harassment policies.

6.15.2 Users are responsible for damages to Computers, SD ECDs, the network, equipment, Electronic Communications Systems, hardware, and software resulting from accidental, negligent, deliberate, and willful acts. Users will also be responsible for incidental or unintended damage resulting from negligent, willful or deliberate violations of this Policy, accompanying administrative regulation, other School District Policies and Other Legal Requirements. For example, Users will be responsible for payments related to lost or stolen Computers SD ECDs and/or School District equipment, and recovery and/or breach of the data contained on them.

6.15.3Violations as described in this Policy, and its accompanying administrative regulation, other School District Policies and Other Legal Requirements may be reported to the School District, to appropriate legal authorities, to the ISPs, websites, or apps, and to local, state, or federal law enforcement. Actions that constitute a crime under state and/or federal law, could result in arrest, criminal prosecution, and/or lifetime inclusion on a sexual offenders registry. The School District will cooperate to the extent legally required with authorities in all such investigations.

6.15.4Vandalism will result in cancellation of access to the School District's CIS Systems and resources and is subject to discipline.

	6.15.5 Any and all costs incurred by the School District for repairs and/or replacement of software, hardware and data files and for technological consultant services due to any violation of this Policy, its accompanying administrative regulation, other School District Policies and Other Legal Requirements shall be paid by the User who caused the loss. If you have questions, contact the Director of Technology at 570-424-8500 x1350. References: PA Consolidated Statutes Annotated – 18 Pa. C.S.A. § 5903, 6312 PA Child Internet Protection Act – 24 P.S. § 4601 et seq. PA Bullying Act – 24 P.S. § 13-1303.1-A PA – 18 Pa. C.S.A. § 6312; 24 P.S. § 4603, 4604 U.S. Copyright Law – 17 U.S.C. § 101 et seq. Digital Millennium Copyright Act 17 U.S.C. § 512, 1202 United States Code – 18 U.S.C. § 1460, 2246, 2252, 2256;47 U.S.C. § 254 Enhancing Education Through Technology Act of 2001 – 20 U.S.C. § 6777 Federal Children's Internet Protection Act – 47 U.S.C. § 254 Board Policies, Administrative Regulations, Rules, and Procedures