SECTION: OPERATIONS

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

DUNMORE SCHOOL DISTRICT

ADOPTED:

REVISED: DECEMBER 14, 2011

815. ACCEPTABLE USE OF THE COMPUTERS, NETWORK, INTERNET, ELECTRONIC COMMUNICATIONS AND INFORMATION SYSTEMS

1. Purpose

The Dunmore School District ("district") provides employees, students, and guests ("users") with hardware, software, access to the school district's electronic communication systems and network, which includes Internet access, whether wired, wireless, virtual, cloud, or by any other means. Guests include, but are not limited to, visitors, workshop attendees, volunteers, independent contractors, adult education staff, students, Board members, vendors, and consultants.

Computers, network, Internet, electronic communications, information systems, databases, files, software, and media (collectively "CIS systems") provide vast, diverse and unique resources. The Board of School Directors will provide access to the school district's CIS systems for users if there is a specific school district-related purpose to access information; to research; to collaborate; to facilitate learning and teaching; and to foster the educational purpose and mission of the school district.

For users, the school district's CIS systems must be used for educational purposes and performance of school district job duties. Incidental personal use (as defined in this policy) of school district computers is permitted for employees. Students may only use the CIS systems for educational purposes. CIS systems may include school district computers which 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 areas or environments, directly from home, or indirectly through another Internet Service Provider (“ISP”), and, if relevant, when users bring and use their own personal computers or personal electronic devices, and, if relevant, when users bring and use another entity’s computer or electronic devices to a school district location, event, or connect it to a school district network.

If users bring personal computers or at the same time, personal technology devices brought onto the district's property, or at district events, or connected to the district's network, that the district reasonably believes contain district information or contain information that violates a district policy, or contains information/data that the district

	reasonably believes involves a criminal activity may be legally accessed to ensure compliance with this policy, other district policies, and to comply with the law. Users may not use their personal computers to access the district's intranet, Internet or any other CIS system unless approved by the Director of Information Systems and/or designee, and/or authorized as part of the district's services for users. The school district intends to strictly protect its CIS systems 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 report immediately any violations or suspicious activities to the Director of Information Systems. Conduct otherwise 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, regulations, rules, and procedures.
2. Definitions 18 U.S.C. Sec. 2256(8) 20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254(h)(7)(F)	**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. Sec. 6312(d) 24 P.S. Sec. 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.
18 U.S.C. Sec. 2256(6) 20 U.S.C. Sec 6777(e)	**Computer** - includes any school district owned, leased or licensed or user-owned personal hardware, software, or other technology device 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. For example, **computer** includes, but is not limited to, the school district's and users': desktop, notebook, power books, tablet PC, iPad, Kindle, eBook readers, 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; RFID; personal digital assistants (PDAs); iPods; MP3 players; thumb drives; cell phones (with or without Internet access and/or recording and/or camera/video and other capabilities and configuration); telephones; mobile phones; or wireless devices; two-way radios/telephones; beepers; paging devices; laser pointers and attachments; Pulse Pens; 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 photo electronic facilities for the transmission/transfer of signs, signals, writings, images, sounds, data, or intelligence of any nature, 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, voice mail services, tweeting, text messaging, instant messaging, GPS, PDAs, facsimile machines, cell phones (with or without Internet access and/or electronic mail and/or recording devices), cameras/video, and other capabilities and configurations. **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. Sec. 6777(e)(6) 47 U.S.C. Sec. 254(h)(7)(G)	**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(e)(6) 24 P.S. Sec. 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; 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.
47 U.S.C. Sec. 254	**Inappropriate Matter** - includes, but is not limited to, visual, graphic, video, text and any other form of indecent, obscene, pornographic, child pornographic, or other material that is harmful to minors, sexually explicit, or sexually suggestive. 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, rude, 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, flagging, terroristic material, and advocating the destruction of property. **Incidental Personal Use** - incidental personal use of school district computers is 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 this policy, all other applicable school district policies, regulations, rules, and procedures, as well as ISP terms, local, state and federal laws, and must not damage the school district's CIS systems.
18 Pa. C.S.A. Sec. 5903(e) 18 U.S.C. Sec. 2256 20 U.S.C. Sec. 6777(e) 47 U.S.C. Sec. 254(h)(7)(D)	**Minor** - for purposes of compliance with the federal 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.

20 U.S.C. Sec. 6777(e) 47 U.S.C. Sec. 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. 3. Whether the work taken as a whole lacks serious literary, artistic, political, educational, or scientific value.
18 Pa. C.S.A. Sec 5903(b) 24 P.S. Sec. 4603	Under Pennsylvania law, analysis of the material meets the following elements: 1. The average person, applying contemporary community standards, would find that the subject 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(e)(3) 18 U.S.C. Sec. 2246 20 U.S.C. Sec 6777(e) 47 U.S.C. Sec. 254(7)(H)	**Sexual Act and Sexual Contact** - as defined at 18 U.S.C. § 2246(2), at 18 U.S.C. § 2246(3), and 18 Pa. C.S.A. § 5903.
24 P.S. Sec. 4604 47 U.S.C. Sec. 254(h)(7)(I)	**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 U.S.C. Sec. 1460(b) 18 U.S.C. Sec. 2256	**Visual Depictions** - includes undeveloped film and videotape and data stored on computer disk or by electronic means which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format but does not include mere words.

3. Authority SC 510 24 P.S. Sec. 4604 47 U.S.C. Sec. 254(1)	Access to the school district's CIS systems through school resources is a privilege, not a right. These, as well as the user accounts and information, are the property of the school district. The school district 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 cooperate to the extent legally required with ISP, local, state and federal officials in any investigation concerning or related to the misuse of the CIS systems. 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 user accounts for any reason in order to uphold this policy, other school district policies, regulations, rules, and procedures, the law, and to maintain the system. 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, 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 and all CIS systems use and to monitor and allocate fileserver space. Users of the school district's CIS systems who transmit or receive communications and information shall be deemed to have consented to having the content of any such communications recorded, checked, received, monitored, tracked, logged, accessed and otherwise inspected or used by the school district, and to monitor and allocate fileserver space. Passwords and message delete functions do not restrict the school district's ability or right to access such communications or information.
24 P.S. Sec. 4604, 4610 20 U.S.C. Sec. 6777(c) 47 U.S.C. Sec. 254	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 on its computers used and accessible to adults and students so as to filter or block inappropriate matter as defined in this policy on the Internet. Measures designed to restrict adults' and minors' access to material harmful to minors may be disabled to enable an adult or student (who has provided written consent from a parent/guardian) to access bona fide research, not within the prohibitions of this policy, or for another lawful purpose. No person may have access to material that is illegal under federal or state law.

24 P.S. Sec. 4604	Expedited review and resolution of a claim that the policy is denying a student or adult to access material will be enforced by an administrator, supervisor, or their designee, upon the receipt of a written consent from a parent/guardian for a student, and upon the written request from an adult presented to the Director of Information Systems. The school district has the right, but not the duty, to inspect, review, or retain electronic communications created, sent, displayed, received, or stored on or over its CIS systems; to monitor, 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, network, 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 network, or when using the school district's mobile computing equipment, telecommunication facilities in 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 electronic devices to a school district location, event, or connect it to a school district network and/or systems, and/or that contains school district programs, or school district or other users' data or information, all pursuant to the law, in order to ensure compliance with this policy and other school district policies, regulations, rules, procedures, ISP terms, and local, state, and federal laws, to protect the school district's resources, and to comply with the law. The school district reserves the right to restrict or limit usage of lower priority CIS systems and computer uses when network and computing requirements exceed available capacity according to the following priorities: 1. Highest - uses that directly support the education of the students. 2. Medium - uses that indirectly benefit the education of the students. 3. Lowest - uses that include reasonable and limited educationally-related interpersonal communications, and limited personal use. 4. Forbidden - all activities in violation of this policy, other school district regulations, rules, and procedures, ISP terms, and local, state and federal laws. The school district additionally reserves the right to: 1. Determine which CIS systems services will be provided through school district resources.

	2. Determine the types of files that may be stored on school district fileservers and computers. 3. View and monitor network traffic, fileserver space, processor, and system utilization, and all applications provided through the network and electronic communications systems, including e-mail and other electronic communications. 4. Remove excess e-mail and other electronic communications or files taking up an inordinate amount of fileserver space after a reasonable time. 5. Revoke user privileges, remove user accounts, or refer to legal authorities and/or school district authorities when violation of this and any other applicable school district policies, regulations, rules, and procedures occur or ISP terms, or local, state or federal law is violated, including, but not limited to, those governing network use, copyright, security, privacy, employment, vendor access, data breaches, and destruction of school district resources and equipment. Due to the nature of the Internet as a global network connecting thousands of computers around the world, inappropriate matter can be accessed through the network and electronic communications systems. Because of the nature of the technology that allows the Internet to operate, the 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, and as provided in other relevant school district policies, regulations, rules, and procedures. Part of the district's Internet safety policy includes educating minors about appropriate online behavior, including interacting with other individuals on social networking web sites and in chat rooms and cyberbullying awareness and response. Users must be capable and able to use the school district's CIS systems and software relevant to their responsibilities. In addition, users must practice proper etiquette, school district ethics, and agree to the requirements of this policy, regulations, rules, and procedures.
4. Delegation of Responsibility	The Director of Information Systems 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, establish a system to ensure adequate supervision of the CIS systems, maintain executed User CIS Acknowledgement and Consent Forms, and interpret and enforce this policy.

	The Director of Information Systems and/or designee will establish a process for setting up individual and class accounts, set quotas for disk usage on the system, establish a records retention and record destruction policies, and records retention schedule to include electronically stored information and establish the school district virus protection process. Unless otherwise denied for cause, student access to the CIS systems resources shall 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 and school district CIS systems, and to abide by the policies, regulations, rules, and procedures established by the school district, its ISP terms and local, state and federal laws.
SC 1303.1-A 47 U.S.C. Sec. 254(5)(B) (iii) Pol. 249	The Director of Information Systems and/or designee(s) has the responsibility to educate minors about appropriate online behavior, including interacting with other individuals on social networking web sites and in chat rooms and cyberbullying awareness and response.
5. Guidelines	<u>Access To The CIS Systems</u> The CIS systems accounts of users must be used only by authorized owners of the accounts and only for authorized purposes. An account will be made available according to a procedure developed by appropriate school district authorities. *CIS System –* This policy, as well as other relevant school district policies, regulations, rules, and procedures, ISP terms, and local, state, and federal laws will govern use of the school district's CIS systems for users. Types of services include, but are not limited to: 1. Internet - School district employees, students, and guests will have access to the web through the district's CIS systems, as needed.

2. E-Mail - District employees may be assigned individual e-mail accounts for work-related use, as needed. Students may be assigned individual e-mail accounts as necessary, by the Director of Information Systems and/or designee and at the recommendation of the teacher who will also supervise the students' use of the e-mail service.

3. Guest Accounts - Guests may receive an individual web account with the approval of the Director of Information Systems, 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 and all other school district policies, regulations, procedures, and rules, as well as ISP terms, local, state and federal laws and may not damage the school district's CIS systems.

4. Blogs - Employees may be permitted to have school district-sponsored blogs after they receive training and the approval of the school district. All bloggers must follow the rules provided in this policy, and other applicable policies, regulations, rules, and procedures of the school district, as well as ISP terms, and local, state, and federal laws.

5. Web 2.0 Second Generation & Web 3.0 Third Generation Web-based Services - Certain school district authorized Second Generation and Third Generation Web-based Services, such as blogging, authorized social networking sites, wikis, podcasts, RSS feeds, social software, folksomonies 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 comply with this policy as well as any other relevant school district policies, regulations, rules, procedures, including copyright, participatory learning/collaboration/social networking, ISP terms, and local, state, and federal laws during such use.

<u>Parental Notification And Responsibility</u>

24 P.S.
Sec. 4604

The school district will notify the parents/guardians about the school district's CIS systems and the policies governing their use. This policy contains 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 a 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. The school district will encourage parents/guardians to specify to their child(ren) what material and matter is and is not acceptable for their child(ren) to access through the school district's CIS system. School District Limitation Of Liability The 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, miss-delivered, or unavailable when using the 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. Prohibitions 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 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 CIS systems. These prohibitions are in effect any time school district resources are accessed whether on school district property, at school district events, connected to the school district's network, when using mobile commuting equipment, telecommunication facilities in unprotected areas or environments, directly from home, or indirectly through another ISP and, if relevant, when a user uses their own equipment.
Pol. 237	Students are prohibited from visually possessing and using their personal electronic devices or their personal computers as defined in this policy, on school district premises property during school hours, unless authorized to do so by administrative staff. At no time may students use their personal electronic devices to connect to the Dunmore School District network without written authorization from the Director of Information Systems. Users are also prohibited from using cell phones, ipods, or any other electronic devices while on

	school property for recording purposes without express permission from Dunmore staff. Students who are performing volunteer fire company, ambulance or rescue squad functions, or who need such a personal electronic device or computer due to their medical condition, or the medical condition of a member of their family, with notice and the approval of the school administrator may qualify for an exemption of this prohibition. <u>General Prohibitions</u> Users are prohibited from using school district CIS systems to: 1. Communicate about nonwork- or nonschool-related communications, unless for incidental personal use as defined in this policy. 2. Send, receive, view, download, store, access, print, post, distribute, or transmit material that is harmful to minors, indecent, obscene, pornographic, child pornographic and terroristic, sexually explicit, sexually suggestive, including but not limited to, visual depictions. 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). Neither may uers advocate the destruction of property. 3. Send, receive, view, download, store, access, print, distribute, or transmit inappropriate matter, as defined in this policy, and material likely to be offensive or objectionable to recipients.
SC 1303.1-A Pol. 249	4. Bullying/Cyberbullying another individual or entity. (See school district bullying policy 249.) 5. Ganging up on a victim or target a person to make that person a subject of ridicule. 6. Access or transmit gambling pools for money, including, but not limited to, basketball and football, or any other betting or games of chance. 7. Participate in discussion or news groups that cover inappropriate and/or objectionable topics or materials, including those that conform to the definition of inappropriate matter in this policy. 8. Send terroristic threats, hateful mail, harassing communications, discriminatory remarks, and offensive, profane, or inflammatory communications.

	9. Participate in unauthorized Internet relay chats, newsgroups, instant messaging communications and Internet voice communications (online; realtime conversations) that are not for school-related purposes or required for employees to perform their job duties. Students must obtain consent from their teacher to use IRC's; however, they may not use instant messaging or text messaging. Employees may only use instant messaging if consent was obtained from the Director of Information Systems and/or designee. 10. Use in an illegal manner or to facilitate any illegal activity. 11. Communicate through e-mail for noneducational purposes or activities, unless for incidental personal use as defined in this policy. 12. Engage in commercial, for-profit, or any business purposes (except where such activities are otherwise permitted or authorized under applicable school district policies); conduct unauthorized fundraising or advertising on behalf of the school district and nonschool district organizations; resell school district computer resources to individuals or organizations; or use the school district's name in any unauthorized manner that would reflect negatively on the school district, its employees or students. **Commercial purposes** are defined as offering or providing goods or services or purchasing goods or services for personal use. School district acquisition policies must be followed for school district purchase of goods or supplies through the school district system. 13. Engage in political lobbying.
Pol. 814	14. Install, distribute, reproduce or use copyrighted software on school district computers, or copy school district software to unauthorized computer systems, intentionally infringing upon the intellectual property rights of others or violating a copyright. (See copyright infringement section in this policy, the school district's copyright policy and the school district's copyright guidelines handbook for additional information.) 15. Plagiarize works that are found on the Internet. **Plagiarism** is taking the ideas or writings of others and presenting them as if they were yours. 16. Install computer hardware, peripheral devices, network hardware, or system hardware. The authority to install hardware or devices on school district computers is restricted to the Director of Information Systems and/or designee.

17. Encrypt messages using encryption software that is not authorized by the school district from any access point on school district equipment or school district property. Users must use school district-approved encryption to protect the confidentiality of sensitive or critical information in the school district's approved manner.

18. Access, interfere, possess, or distribute confidential or private information without permission of the school district's administration. An example includes accessing other students' accounts to obtain their grades, or accessing other employees' accounts to obtain information.

19. Violate the privacy or security of electronic information.

20. Send any school district information to another party, except in the ordinary course of business as necessary or appropriate for the advancement of the school district's business or educational interest.

21. Send unsolicited commercial electronic mail messages, also known as spam.

22. Post personal or professional web pages on the school district's web site without approval.

23. Post anonymous messages.

24. Use the name of the Dunmore School District in any form on school district Internet pages or web sites, on web sites not owned or related to the school district, or in forums/discussion boards, and on social networking web sites to express or imply the position of the Dunmore School District without the expressed, written permission of the Superintendent. School-affiliated organizations, including booster clubs and parent-teacher organizations, would be exempt from this provision.

25. Bypass or attempt to bypass Internet filtering software by any method, including, but not limited to, the use of anonymizers/proxies or any web sites that mask the content the user is accessing or attempting to access.

26. Advocate illegal drug use, whether expressed or through a latent pro-drug message. This does not include a restriction of political or social commentary on issues.

27. Attempt to and/or obtain personal information under false pretenses with the intent to defraud another person.

28. Use location devices to harm another person.

29. Post false statements, or assume the identity of another person.

Access And Security Prohibitions

Users must immediately notify the Director of Information Systems and/or designee if they have identified a possible security problem. Users must read, understand, and submit an electronically or written signed CIS Acknowledgement and Consent Form(s), and comply with this policy that includes network, Internet usage, electronic communications, telecommunications, nondisclosure and physical and information security policies.

The following activities related to access to the school district's CIS systems 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. Users are required to use unique, strong passwords that comply with the school district's password, authentication, and syntax requirements. Users will be held responsible for the result of any misuse of users' names or passwords while the users' systems access were left unattended and accessible to others, whether intentional or whether through negligence.

3. Using or attempting to use computer accounts of others.

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.

	8. Accessing any web site that the school district has filtered or blocked as unauthorized. Examples include, but are not limited to, unauthorized social networking, music download, and gaming sites.
Pol. 830	9. Users must protect and secure all electronic resources and information, data and records of the school district from theft and inadvertent disclosure to unauthorized individuals or entities when they are under the supervision and control of the school district, and when they are not under the supervision and control of the school district, for example, but not limited to, working at home, on vacation or elsewhere. If any user becomes aware of the release of school district information, data or records, the release must be reported to the Director of Information Systems immediately. (See the district's data breach policy 830 for further information.) <u>Operational Prohibitions</u> The following operational activities and behaviors are prohibited: 1. Interference with, infiltration into, or disruption of the CIS systems, network accounts, services or equipment of others, including, but not limited to, the propagation of computer "worms" and "viruses", Trojan Horse, trapdoor, robot, spider, crawler, and other program code; the sending of electronic chain mail, 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 spyware designed to steal information, or viruses and worms or other hardware or software designed to damage the CIS systems, 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 CIS systems 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 retransmission of any computer, electronic communications systems, or network services, whether wired, wireless, cable, virtual, cloud, or by other means.

6. Connecting unauthorized hardware and devices to the CIS systems.

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

11. Damaging the school district's computers, CIS systems, networking equipment through the users' negligence or deliberate act, including, but not limited to, vandalism.

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

<u>Content Guidelines</u>

Information electronically published on the district's CIS systems 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 date of birth, Social Security number, driver's license number, financial information, credit card number, health information, phone number(s), 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.

4. Documents, web pages and electronic communications, must conform to all school district policies, regulations, rules, and procedures.

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 ISP terms, and local, state, and federal officials to the extent legally required in investigations concerning or relating to any illegal activities conducted through the school district's CIS systems.

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

Users' violations of this policy, any other school district policies, regulations, rules, and procedures, ISP terms, or the law may be discovered by routine maintenance and monitoring of the school district's system, or any method stated in this policy, or pursuant to any legal means.

The school district reserves the right, but not the duty, to inspect, review, or retain electronic communications created, sent, displayed, received, or stored on or over its CIS systems; to monitor, record, check, track, log, access, or otherwise inspect; and/or report all aspects of its CIS systems. This includes any personal computers, network, Internet, electronic communications systems, databases, files, software, and media that they bring onto the school district's property, or to school district's events, that were connected to the school district network, and/or that contain school district programs, or school district or users' data or information, all pursuant to law, in order to ensure compliance with this policy, other school district policies, regulations, rules, and procedures, ISP terms, and local, state, and federal law in order to protect the school district's resources, and to comply with the law.

Everything that users place in their personal files should be written as if a third party will review it.

	Copyright Infringement And Plagiarism
17 U.S.C. Sec. 101 et seq Pol. 814	Federal laws, cases, policies, and guidelines pertaining to copyright will govern the use of material accessed through the school district resources. (See school district copyright 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 comply with the fair use doctrine, and/or 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 his/her own risk and assumes all liability. Violations of copyright law include, but are not limited to, 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, remixing and preparing mash-ups, and deep-linking and framing into the content of others' web sites. Further, the illegal installation of copyrighted software or files for use on the school district's computers is expressly prohibited. This includes all forms of licensed software: shrink-wrap, click wrap, browse wrap, and electronic software downloaded from the Internet.
17 U.S.C. Sec. 1202	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. School district guidelines on plagiarism will govern use of material accessed through the school district's CIS systems. Users must not plagiarize works that they find. Teachers will instruct students in 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. Selection Of Material School district policies on the selection of materials will govern use of the school district's CIS systems.

	When using the Internet for class activities, teachers must select material that is appropriate in light of the age of the students and that is relevant to the course objectives. Teachers will preview the materials and web sites they require or recommend students access to determine the appropriateness of the material contained on or accessed through the web site. Teachers must provide guidelines and lists of resources to assist their students in channeling their research activities effectively and properly. Teachers must 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. School District Web Site The school district will establish and maintain a web site and will develop and modify its web pages that will present information about the school district under the direction of the Director of Information Systems and/or designee. Publishers must comply with this policy and other school district policies, regulations, rules, and procedures; for example, the school district's web site development policy, ISP terms, and local, state, and federal laws.
17 U.S.C. Sec. 512	The school district may limit its liability by complying with the Digital Millennium Copyright Act's safe harbor notice and takedown provisions. Blogging If an employee, student or guest creates a blog with their own resources, the employee, student, or guest may not violate the privacy rights of employees and students, may not use school district personal and private information/data, images and copyrighted material in their blog, and may not disrupt the school district. Conduct otherwise will result in actions further described in the Consequences for Inappropriate, Unauthorized and Illegal Use section of this policy and provided in relevant school district policies, regulations, rules, and procedures. Safety And Privacy 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 unwelcome communications must immediately send or take them to the Director of Information Systems and/or designee.

Users will not post 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, and other program codes; or may not use school district or personal technology or resources in any way to invade one's privacy. Additionally, users may not disclose, use or disseminate confidential and personal information about students or employees. Examples include, but are not limited to, revealing biometric data, revealing 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 district, by using a PDA, iPhone, Blackberry, cell phone (with or without camera/video) and/or other computer, unless legitimately authorized to do so.

If the school district requires that data and information be encrypted, users must use school district authorized encryption to protect their security.

Student users will agree not to meet with someone they have met online unless they have parental consent.

Consequences For Inappropriate, Unauthorized And Illegal Use

General rules for behavior, ethics, and communications apply when using the CIS systems and information, in addition to the stipulations of this policy, other school district policies, regulations, rules, and procedures, ISP terms, and local, state, and federal laws. Users must be aware that violations of this policy or other school district policies, regulations, rules, and procedures or for unlawful use of the CIS systems, may result in loss of CIS 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), dismissals, expulsions, breach of contract, and/or legal proceedings on a case-by-case basis. This policy incorporates all other relevant school district policies, such as, but not limited to, the student and professional employee discipline policies, Code of Student Conduct, copyright, property, curriculum, terroristic threat, and harassment policies.

Users are responsible for damages to computers, the network, equipment, electronic communications systems, 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, other school district policies, regulations, rules, and procedures, ISP terms,

and local, state, and federal laws. For example, users will be responsible for payments related to lost or stolen computers and/or school district equipment, and recovery and/or breach of the data contained on them.

Violations as described in this policy, other school district policies, regulations, rules, and procedures may be reported to the school district and to appropriate legal authorities, whether the ISP, local, state, or federal law enforcement, and may constitute a crime under state and/or federal law which may 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.

Vandalism will result in cancellation of access to the school district's CIS systems and resources and is subject to discipline. **Vandalism** is defined as any malicious attempt to harm or destroy data of another user, Internet or other networks; this includes, but is not limited to, uploading or creating computer viruses.

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, other school district policies, regulations, rules, and procedures, or ISP, local, state or federal law must be paid by the user who causes the loss.

References:

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

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.

Digital Millennium Copyright Act – 17 U.S.C. Sec. 512, 1202

Obscenity – 18 U.S.C. Sec. 1460

Sexual Abuse – 18 U.S.C. Sec. 2246

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, 103.1, 104, 218, 218.2, 220, 233, 237, 248, 249, 317, 348, 417, 448, 517, 548, 814, 830