SECTION: OPERATIONS

TITLE: ACCEPTABLE USE OF INTERNET, TECHNOLOGY, COMPUTERS, AND NETWORK RESOURCES

LACKAWANNA TRAIL SCHOOL DISTRICT

ADOPTED: JULY 2012

REVISED: MARCH 2014

	815. ACCEPTABLE USE OF INTERNET, TECHNOLOGY, COMPUTERS, AND NETWORK RESOURCES
1. Purpose	The Board supports the use of the District's Internet, technology, computers and network resources to facilitate teaching and learning, to provide access to information, to aid in research and collaboration, to foster the educational mission of the District, and to carry out the legitimate business and operation of the District. The District provides its employees, students, and guests ("users") access to Internet, technology, computers and network resources including, but not limited to, electronic communications systems, computers, computer networks, networked devices, hardware, software, Internet access, mobile devices, peripherals, copiers, and cameras. The use of the District's Internet, technology, computers and network resources is for appropriate school-related educational and operational purposes and for the performance of job duties consistent with the educational mission of the District. Use for educational purposes is defined as use that is consistent with the curriculum adopted by the District, as well as, the varied instructional needs, learning styles, abilities and developmental levels of students. All users for any purpose must comply with this policy and all other applicable codes of conduct, policies, procedures, and rules and must not cause damage to the District's Internet, technology, computers and network resources. All employees and students are responsible for the appropriate and lawful use of the District's Internet, technology, computers and network resources. This policy is intended to ensure that all users continue to enjoy access to the District's Internet, technology, computers and network resources and that such resources are utilized in an appropriate manner and for legitimate purposes. This Board policy is provided so users are aware of their responsibilities when using the District's Internet, technology, computers and network resources and to explain to users that they will be held accountable for noncompliance with this policy.

2. Authority	The Board establishes that access to and use of the District's Internet, technology, computers and network resources is a privilege, not a right, which may be revoked at any time. The District's Internet, technology, computers and network resources are the property of the District. The District provides these resources for educational and operational purposes as stated herein and are not provided as a public access service or to provide a public forum. The Superintendent or designee is responsible for overseeing the District's Internet, technology, computers and network resources. The Superintendent will designate a network administrator who will serve as the coordinator and supervisor of these resources and who will work with other regional and state organizations as necessary to educate users, approve activities, provide leadership for proper training of all users in the use of the District's Internet, technology, computers and network resources and the requirements of this policy, and who will establish a system to ensure that users who access the District's Internet, technology, computers and network resources have agreed to abide by the terms of this policy. The Superintendent or designee is directed to implement Internet safety measures to effectively address the following, both through general policy and through the use of filtering technology: 1. Access by minors to inappropriate or harmful content. 2. Safety and security of minors when using electronic mail, chat rooms, and social networking. 3. Prevention of unauthorized access of District Internet, technology, computers and network resources. 4. Prevention of unauthorized disclosure and dissemination of minors' personal information.
3. Definitions 18 U.S.0 Sec. 2256	User shall mean anyone who utilizes or attempts to utilize the District's Internet, technology, computers and network resources while on or off District property. The term includes, but is not limited to, students, staff, parents/guardians, and any visitors to the District that may use the District's Internet, technology, computers, and network resources. **Internet, Technology, Computer, and Network Resources** shall include all technology owned and/or operated by the District, including computers, projectors, televisions, video and sound systems, mobile devices, calculators, scanners, printers, cameras, portable hard drives, hardware, software, routers, and networks, including the Internet.

	The term child pornography is defined under both federal and state law. **Child pornography,** under federal law, is any visual depiction, including any photography, 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 visual 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	**Child pornography,** under state law, is 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. The term harmful to minors is defined under both federal and state law.
20 U.S.0 Sec. 6777 47 U.S.C. Sec. 254	**Harmful to minors,** under federal law, is any picture, image, graphic image file or other visual depiction that: 1. Taken as a whole, with respect to minors, appeals to a prurient interest in nudity, sex or excretion; 2. Depicts, describes or represents in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or lewd exhibition of the genitals; and 3. Taken as a whole lacks serious literary, artistic, political or scientific value as to minors.
18 Pa. C.S.A. Sec. 5903	**Harmful to minors,** under state law, is 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.
18 Pa. C.S.A. Sec. 5903	Obscene is any material or performance, if 1. The average person applying contemporary community standards would fmd 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.
47 U.S.C. Sec. 254	**Technology protection measure** is a specific technology that blocks or filters Internet access to visual depictions that are obscene, child pornography or harmful to minors.
Pol. 218, 233, 317	The Board declares that Internet, technology, computers, and network resource use is a privilege, not a right. The District's Internet, technology, computers and network resources are the property of the District. Users shall have no expectation of privacy in anything they create, store, send, delete, receive or display on or over the District's Internet, technology, computers, or network resources, including personal files or any use of the District's Internet, technology, computers, and network resources. The District reserves the right to monitor, track, and log network access and use; monitor fileserver space utilization by District users; or deny access to prevent unauthorized, inappropriate or illegal activity and may revoke access privileges and/or administer appropriate disciplinary action. The District shall cooperate to the extent legally required with the Internet Service Provider (ISP), local, state and federal officials in any investigation concerning or related to the misuse of the District's Internet, technology, computers, and network resources. The Board requires all users to fully comply with this policy and to immediately report any violations or suspicious activities to the Superintendent or designee.
47 U.S.C. Sec. 254	The Board establishes the following materials, in addition to those stated in law and defined in this policy, that are inappropriate for access by minors: 1. Defamatory. 2. Lewd, vulgar, or profane. 3. Threatening.

Pol. 103, 103.1, 104, 248, 348	4. Harassing or discriminatory.
Pol. 249	5. Bullying.
Pol. 218.2	6. Terroristic.
	7. Others.
4. Delegation of Responsibility Pol. 226, 237	The District shall make an effort to ensure that the District's Internet, technology, computers and network resources are used responsibly by students and staff and that it is consistent with its educational and professional purposes. Users of electronic and personal communication devices shall, prior to being given access, sign user agreements acknowledging awareness of the provisions of this policy and of policy 237, and awareness that the District uses systems to monitor and detect inappropriate use, and may use tracking systems to track and recover lost or stolen equipment. In the case of a minor student, user agreements shall also be signed by a parent/guardian.
47 U.S.C. Sec. 254 SC 1303.1-A Pol. 249	The Board directs that the Superintendent or designee educate students at all levels with respect to Internet, technology, computers, and network resources. This includes teaching students network etiquette and other appropriate online behavior including interacting via social networks and in chat rooms, cyber-bullying prevention, and nondisclosure of personal information, as well as, helping students develop the intellectual skills necessary to discern among information sources, identify information appropriate to their age and developmental levels, and evaluate and use the information to meet their educational goals.
24 P.S. Sec. 4604	The Superintendent or designee shall annually notify students, staff, and parents/guardians about the District's Acceptable Use of Internet, Technology, Computers and Network Resources policy via the student/staff handbooks, District's website, and other efficient methods. A copy of this policy shall be provided to parents/guardians, upon written request. Students, staff, and other authorized individuals have the responsibility to respect and protect the rights of every other user in the District and on the Internet. Building administrators shall make initial determinations of whether inappropriate use has occurred.
20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254 47 CFR Sec. 54.520	The Superintendent or designee shall be responsible for recommending technology and developing procedures used to determine whether the District's Internet, technology, computers and network resources are being used for purposes prohibited by law or for accessing sexually explicit materials. The procedures shall include but not be limited to:

	1. Utilizing a technology protection measure that blocks or filters Internet access for minors and adults to certain visual depictions that are obscene, child pornography, harmful to minors with respect to use by minors, or determined inappropriate for use by minors by the Board. 2. Maintaining and securing a usage log. 3. Monitoring online activities of minors.
5 Guidelines	<u>Unauthorized Use Prohibited</u> Network accounts shall be used only by the authorized user of the account for its approved purpose. Users are prohibited from sharing their account with others. In the event that a person utilizes an account belonging to another user in violation of the law, District policy or handbook, both users may be liable for consequences resulting from those actions. Network users shall respect the privacy of other users on the system. Only users who have agreed to abide by the terms of this policy may utilize the District's Internet, technology, computers, and network resources. Unauthorized use, utilizing another user's District account, or exceeding one's authorization to use District Internet, technology, computers and network resources is prohibited. <u>District Provided Resources</u> District Internet, technology, computers and network resources may be assigned or allocated to an individual user for his or her use (e.g. individual e-mail accounts, laptop computers, etc.) Despite being allocated to a particular user, the Internet, technology, computers and network resources remain the property of the District and may be revoked, suspended, or inspected at any time to ensure compliance with law, this and other District policies, and handbooks. Users do not have an expectation of privacy with regard to the District's Internet, technology, computers, network resources or any of its contents.
Pol. 237	<u>Use of Personal Electronic Devices</u> The use of electronic and personal communication devices on the District's network is permitted only on designated networks. When a user connects a personal electronic device to a District network or District Internet, technology, computers and network resources, this policy and its guidelines apply. Users are subject to the same levels of monitoring and access as if a District-owned device were being utilized. Users who connect an electronic or personal communication device to a District network explicitly waive any expectation of privacy in the content exchanged over the District's Internet, technology, computers and network resources. <u>Internet Filtering and CIPA Compliance</u> The District utilizes content and message filters to prevent users from accessing

	material through the District's Internet, technology, computers and network resources that has been determined to be obscene, offensive, pornographic, harmful to minors, or otherwise inconsistent with the District's educational mission. The Superintendent or designee shall establish a procedure for users to request that a legitimate website or educational resource not be blocked by the District's filters for a bona fide educational purpose. Such requests must be either granted or rejected within a week pursuant to the established procedure. <u>Safety</u> It is the District's goal to protect users of the network from harassment and unwanted or unsolicited communication. Any network user who receives threatening or unwelcome communications or inadvertently visits or accesses an inappropriate site shall report such immediately to a teacher or administrator. Network users shall not reveal personal information to other users on the network, including chat rooms, email, social networking websites, etc. Any District computer/server utilized by students and staff shall be equipped with Internet blocking/filtering software.
47 U.S.0 Sec. 254 47 CFR Sec. 54.520	Internet safety measures shall be used to address the following: 1. Control of access by minors to inappropriate matter on the Internet. 2. Safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications. 3. Prevention of unauthorized online access by minors, including "hacking" and other unlawful activities. 4. Unauthorized disclosure, use, and dissemination of personal information regarding minors. 5. Restriction of minors' access to materials harmful to them. <u>School District Limitation of Liability</u> The District makes no warranties of any kind, either expressed or implied, for the services it is providing through its various Internet, technology, computers and network resources. The District does not warrant that the functions or the services provided by or through the District's Internet, technology, computers and network resources will be error-free or without defect. The District does not warrant the effectiveness of Internet filtering. The electronic information available to users does not imply endorsement of the content by the District, nor is the District responsible for the accuracy or quality of the information obtained through or stored on the Internet, technology, computers and network resources. The District shall not be responsible for any damages, including loss of data resulting from delays, missed

	deliveries, or service interruption. The District shall not be responsible for material that is retrieved through the Internet, or the consequences that may result. The District shall not be responsible for any fmancial obligations, charges or fees resulting from access to its Internet, technology, computers and network resources. <u>Prohibitions</u> Users are expected to act in a reasonable, ethical and legal manner in accordance with federal and state law, District policy, accepted rules of network etiquette, and building rules when using the District's Internet, technology, computers and network resources. Specifically, the following uses are prohibited: 1. Violating the law, facilitating illegal activity, or to encouraging others to do so; 2. Violating any other District policy; 3. Engaging in any intentional act which might threaten the health, safety, or welfare of any person or persons; 4. Causing, or threatening to cause harm to others or damage to their property; 5. Commercial purposes or for-profit purposes; 6. Engaging in non-professional/non-academic Internet access (ex. Online shopping, travel reservations, gambling, unauthorized sites, etc.) 7. Political lobbying or campaigning, not including student elections (e.g. student government, club officers, homecoming queen, etc.); 8. Tethering or otherwise connecting to a non-District owned device to access an unfiltered and/or unmonitored Internet connection; 9. Bullying/Cyber-bullying, or communicating terroristic threats, discriminatory remarks, or hate; 10. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials;
17 U.S.C. Sec. 101 et seq Pol. 814	11. Communicating words, photos, videos, or other depictions that are obscene, indecent, vulgar, rude, profane, or that advocate illegal drug use; 12. Creating, accessing, or to distributing obscene, profane, lewd, vulgar, pornographic, harassing, or terroristic material;
Pol. 237	13. Attempting to interfere with or disrupt District technology systems, networks, services, or equipment including, but not limited to, the propagation of computer

	"viruses" and "worms", Trojan Horse and trapdoor program codes; 14. Altering or attempting to alter other users' or system files, system security software, system or component settings, or the systems themselves, without authorization; 15. Attempting to physically harm or destroy the District's Internet, technology, computers and network resources; 16. Jeopardizing the security of the District's Internet, technology, computers and network resources, or attempting to circumvent any system security measures; 17. Concealing or attempting to conceal a user's identity, including the use of anonymizers, or the impersonation of another user; 18. Intentionally obtaining or modifying files, passwords, and/or data belonging to other users or to the District; 19. Sending any District information to another party, except in the ordinary course of business as necessary or appropriate for the advancement of the District's business or educational interests; 20. Committing plagiarism or assisting others in committing plagiarism; 21. Installing, loading, or running software programs, applications, or utilities not explicitly authorized by the District technology staff; 22. Installing unauthorized computer hardware, peripheral devices, network hardware, or system hardware onto Internet, technology, computers and network resources; 23. Copying District software without express authorization from a member of the District's technology staff; 24. Unauthorized access, interference, possession, or distribution of confidential or private information without authorization; 25. Using proxies or other means to bypass or disable Internet content filters and monitoring; 26. Accessing a restricted system or changing settings or access rights to a restricted system or account without authorization; 27. Using encryption software that has not been previously approved by the District; 28. Sending unsolicited mass-email messages, also known as spam;

	29. Scanning the District's Internet, technology, computers and network resources for security vulnerabilities; 30. Accessing material that is harmful to minors or is determined inappropriate for minors in accordance with laws, Board policy or building rules; 31. Using inappropriate language or profanity; 32. Transmitting material that is offensive or objectionable to recipients; 33. Disrupting the work or other users; <u>Security</u> System security is protected through the use of passwords. Failure to adequately protect or update passwords could result in unauthorized access to personal or District files. To protect the integrity of the system, the following guidelines shall be followed: 1. Employees and students shall not reveal their passwords to another individual. 2. Users are not to use a computer that is logged in under another student's or employee's name. 3. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the network. <u>District Website</u> The District shall establish and maintain a website and shall develop and modify its web pages to present information about the District under the direction of the Superintendent or designee. All users publishing content on the District website shall comply with this and other applicable District policies, regulations and procedures. Users shall not copy or download information from the District website and disseminate such information on unauthorized web pages without authorization from the building principal. <u>Consequences For Inappropriate Use</u> Violations of this policy may result in the temporary or permanent revocation of a user's right to access District Internet, technology, computers and network resources.
24 P.S. Sec. 4604	The network user shall be responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts. Illegal use of the network; intentional deletion or damage to files of data belonging to others; copyright violations; and theft of services will be reported to the appropriate legal authorities for possible prosecution.

	General rules for behavior and communication apply when using the Internet, in addition to the stipulation of this policy. Additionally, students may be subject to other forms of disciplinary actions for violations of this policy and/or local, state, and/or federal law. Vandalism will result in loss of access privileges, disciplinary action, and/or legal proceedings. **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. <u>Administration/Faculty/Staff Email Use:</u> • Limited to professional/educational communication. • Mass emails are to be used with prior approval of the building principal or Superintendent, unless they are of an academic nature. • Responses to mass emails are to be replies to the sender, not the entire group to which it was sent. • All email activity is subject to administrative review and is not private. • All e-mails will be archived for a period of time determined by the District or as required by law. • Building Administrators may establish their own email guidelines. • Loss of access and other disciplinary actions shall be consequences for failure to adhere to this policy.
Pol. 218, 233, 317	<u>Loss of Privileges</u> Failure to comply with this policy or inappropriate use of the District's Internet, technology, computers, and network resources shall result in usage restrictions, loss of access privileges, disciplinary action, and/or legal proceedings. References: School Code — 24 P.S. Sec. 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. 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, 814