LEWISBURG AREA SCHOOL DISTRICT

SECTION: OPERATIONS

TITLE: ACCEPTABLE USE OF COMPUTER NETWORKS

ADOPTED: February 27, 1997

REVISED: September 26, 2013

815. ACCEPTABLE USE OF COMPUTER NETWORKS

1. Purpose

The Board recognizes that the Lewisburg Area School District computer network, including the Internet and e-mail, is an important resource for facilitating the exchange of information to further daily operations, communications, education, and research and is consistent with the mission of the school district. For instructional purposes, the use of network resources shall be consistent with the adopted school district curriculum as well as the varied instructional needs, learning styles, abilities, and developmental levels of students.

The district computer network includes all local area networking and wide area networking within the school community as well as all on-line and direct-wired networking, such as the Internet, to which the school network may be linked.

2. Authority

The district does not endorse any content accessible through the use of the network facilities, nor does the district guarantee the accuracy of information received. The district shall not be responsible for or restore any information that may be lost, damaged or unavailable when using the network or for any information that is retrieved via the Internet. The district reserves the right to reimage any district computer at its discretion. The district also reserves the right to examine the contents of any district computer at is discretion and without notice.

The school district shall not be responsible for any unauthorized charges or fees resulting from Internet use. Users will be responsible to indemnify the district for any and all claims, lawsuits, causes of action, damages, judgments, losses, expenses, liabilities, or costs associated with a violation of the Acceptable Use of Computer Networks policy without limitation. All users of the district network and district owned computer hardware, software, and equipment shall be bound by this policy.

20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254	The hardware, software, messages transmitted, and documents created on the network are the property of the district. Network users should be aware that computer files and communications over the district network, including e-mail and voice mail, are not private. Under no circumstances shall there be any expectation of privacy when using any district systems. The district has the right to supervise the use of school property, including the hardware, software, messages transmitted, and documents created on the network. The district reserves the right to log network use and to monitor fileserver space utilization by district users. It may be necessary to access user accounts in order to perform routine maintenance and security tasks. The system administrator has the right to access user accounts to uphold this policy and maintain the system. The district reserves the right to remove a user account from the network to prevent unauthorized or illegal activity. District network resources are subject to retrieval and review by the district at any time without further notice to students or staff. The district reserves its right to inspect and examine any use of the district systems; this includes but is not limited to, a user's internet access, e-mail transmissions, and all system registries. Student access to the Internet other than through network and equipment resources provided by the LASD is prohibited on school property. Any use of the district network and equipment without authorization is prohibited. Furthermore, the Board emphasizes that access to the Internet and other computer networks is a privilege, not a right; inappropriate use will result in the cancellation of these privileges and/or appropriate disciplinary action and criminal or civil prosecution where appropriate.
47 U.S.C. Sec. 254	The Board shall establish a list of materials, in addition to those stated in law, that are inappropriate for access by minors. The district also reserves the right to: 1. Specify who uses its equipment and the information contained therein, under what circumstances, and to what purposes. 2. Prohibit the use of district equipment and software by students or staff for private or personal business and will subject the violator to disciplinary action. 3. Determine which technology services will be provided through district resources.

	4. Determine the types of files that may be stored on district file servers and computers. 5. View and monitor network traffic, file server space, processor, and system utilization, and all applications provided through the network and communications systems, including e-mail and other electronic communications. 6. Remove excess e-mail or files taking up an inordinate amount of fileserver disk space after a reasonable time. 7. Revoke user privileges, remove user accounts, or refer to legal and/or district authorities when violation of this and any other applicable district policies occur or state or federal law is violated, including, but not limited to, those governing network use, copyright, security, privacy, employment, and destruction of district resources and equipment.
3. Delegation of Responsibility	Administrators, teachers, and staff have a professional responsibility to work together to help students develop the intellectual skills necessary to discriminate among information resources, to identify information appropriate to their age and developmental levels, and to evaluate and use the information to meet their educational goals. Students and staff have the responsibility to respect and protect the rights of every other user in both the district and on the Internet generally. The building administrator shall have the authority to determine what is inappropriate use.
20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254 47 CFR Sec. 54.520	The Board authorizes the Superintendent and his/her designee's discretion in determining appropriate usage of computer networks within the district and designated buildings. The Superintendent or designee shall be responsible for recommending and developing procedures used to determine whether the district's network and equipment is being used for purposes prohibited by law or for accessing sexually explicit materials. The procedure shall include but not be limited to: 1. Utilizing technology protection measures that block or filter Internet access for minors and adults to information and certain visual depictions that are obscene as defined by law and in this policy, pornographic, harmful to minors with respect to use by minors, or determined to be inappropriate for use by minors by the Board.

	2. Maintaining and securing a usage log. 3. Monitoring online activities of minors.
47 U.S.C. Sec. 254	The Superintendent or designee shall develop and implement administrative regulations that ensure students are educated on network etiquette and other appropriate online behavior, including: 1. Interaction with other individuals on social networking websites and in chat rooms.
SC 1303.1-A Pol. 249	2. Cyberbullying awareness and response.
4. Guidelines	All students and staff will be permitted to use district network resources in furtherance of the mission of the school district. An internet/computer network exemption form shall be made available to parents/guardians that choose to prohibit their child's internet access. As the student matriculates from one school building to the next, the parent/guardian shall submit the internet/network exemption form if they choose to prohibit their child's access. This policy shall be published or referenced annually in the student and staff handbooks. Network accounts shall be used only by the authorized owner of the account for its approved purpose. All communications and information accessible via the network should be assumed to be private property and shall not be disclosed. Network users shall respect the privacy of other users on the network. Users are not to access the district's intranet, its owned or leased technological resources, or the district's internet access while utilizing another user's personal access information. Users are given their own personal ID. Users are responsible for maintaining the privacy of their passwords. Users are responsible for their own individual accounts and should take reasonable precautions to prevent others from using their account. Users must log off or lock the computer when finished or when leaving their workstation. Users are only to sign on to the network with the ID assigned to them. Users will represent only themselves on the network and will only attempt to modify files or passwords belonging to them. Misuse of passwords, unauthorized copying of another's work, and attempting to access files maintained by others is strictly forbidden.

When a user is no longer employed by the district or is no longer a student of the district, their account will be deleted or suspended. Special circumstances may be approved by the Superintendent for accounts to be maintained for a defined period of time.

Each user issued a laptop shall be responsible for the security and care of that laptop, regardless of whether the laptop is used in the district, at the user's place of residence, or in any other location such as a hotel, conference room, car or airport.

Users shall be responsible for all content on their district issued laptop. All district computer and laptop content may be monitored by the district.

Student users are not permitted to install software or alter the operating system without the permission of the technology department.

Parental Notification and Responsibility

The district will notify the parents/guardians about the school district's network and the policies governing its 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 district recognized that parent/guardians bear primary responsibility for transmitting their particular set of family values to their children. The 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 district's network.

Prohibitions

Students and staff are expected to act in a responsible, ethical and legal manner in accordance with district policy, accepted rules of network etiquette, and federal and state law. These prohibitions are in effect any time district resources are accessed whether on district property, at district events, connected to the district's network, directly from home or indirectly through another Internet Service Provider.

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

	The 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 network; to monitor, record, check, track, log, access, or otherwise inspect; and/or report all aspects of its network. This includes computers, network, Internet, electronic communications systems, databases, files, software, and media that they bring onto the district's property, or to district events, that were connected to the district network, and/or that contain district programs, or district/users' data or information, all pursuant to law, in order to ensure compliance with this, other district policies, and local, state, and federal law in order to protect the district's resources, and to comply with the law. Users should understand that there should be no reasonable expectation of privacy with respect to any of the District's technology resources, including but not limited to networks, accounts, hardware, etc. Everything that users place in their personal files should be written as if a third party will review it. Specific prohibited uses include, but are not limited to, the following: 1. Facilitating illegal activity. 2. Engaging in activity which is for commercial, for-profit, or for any other business purpose (except where such activities are otherwise permitted or authorized under applicable district policies); conducting unauthorized fundraising or advertising on behalf of the district and nonschool organizations; reselling of district computer resources to individual or organizations who are not related to the district; or use of the district's name in any unauthorized manner that would reflect negatively on the district, its employees, or students. **Commercial purposes** are defined as offering or providing goods or services or purchasing goods or services for personal use. 3. Use which is not school or work related, except for incidental personal use. E-mail is not to be used for the mass mailing of noneducational or nonwork related information or for the sending of unsolicited commercial electronic mail messages, commonly known as spam. 4. Product advertisement or political lobbying, except for teacher's association business as outlined in the collective bargaining agreement.
SC 1303.1-A Pol. 249	5. District resources shall not be used for bullying/cyberbulling, sending terroristic threats, hateful mail, harassing communications, making discriminatory remarks, and all other harassing, offensive, or inflammatory remarks.

	6. Accessing or distributing material of a profane, discriminatory, threatening (including hate mail), offensive, or inflammatory nature.
Pol. 814	7. Reproducing, distributing, communicating, installing, or modifying materials in violation of copyright laws or fair use guidelines.
Pol. 237	8. Access, obtain, or distribute materials, images, or photographs that are obscene, pornographic, lewd, constitute child pornography as defined herein, or are otherwise illegal.
	9. Access by students, faculty, and guests to material that is harmful to minors or is determined inappropriate for minors in accordance with Board policy.
	10. Inappropriate language or profanity.
	11. Accessing or transmitting material likely to be offensive or objectionable to recipients, including but not limited to, that which may be defamatory, inaccurate, obscene, sexually explicit, lewd, hateful, 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, vulgar, rude, inflammatory, threatening, profane, pornographic, offensive, terroristic, and/or otherwise illegal.
	12. Infiltrating a computing system, tampering with network hardware or software (including viruses), gaining unauthorized access into password protected areas of the network, attempting to by-pass the district's filtering software, intentionally obtaining, modifying, vandalizing or destroying network files or data belonging to or used by others, or other behavior that interferes with the functioning of the district network.
	13. Impersonating another user, maintaining anonymity, using pseudonyms, or gaining or attempting to gain network access through fraudulent means.
	14. Loading or using unauthorized games, program files, music, or other electronic media, pirated software, and peer-to-peer file-sharing software. Network users will not download files unless instructed to do so by a teacher who has obtained authorization from the Superintendent or his/her designee.
	15. Disrupting the work of other users.
	16. Quoting of personal communications in a public forum without the original author's prior consent.

17. Transmitting confidential information about students, employees or district operations without administrative authority.

18. Access and use of online "gaming" sites (except for approved educational purposes).

19. Accessing or transmitting any form of gambling, including but not limited to, basketball and football pools, online poker websites, and any other form of betting, gambling, or games of chance.

20. Access to "social networking" sites for noncurricular purposes, including participation in unauthorized Internet Relay Chats, instant messaging communications and Internet voice communications (on-line, real-time conversations) that are not for school-related purposes or required for employees to perform their job duties.

21. Participation 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.

22. Accessing, interfering, possessing, or distributing confidential or private information without permission from the district administration, e.g. accessing another student's account to obtain their grades. Users may not violate the privacy or security of electronic information contained on the network.

23. Distributing or publishing a password, identifying code, personal identification number, username, or any other confidential information about a computer, computer system, network, or e-mail account or database.

Operational Prohibitions

The following activities, behaviors, and operations are prohibited:

1. Interference with or disruption of the district systems, network accounts, services or equipment through, but not limited to, the propagation of computer "worms" and "Viruses," Trojan Horses, and trapdoor program code. The user may not hack or crack the network or others' computers, whether by parasite ware or spyware designed to steal information; phishing; viruses and worms; other hardware or software designed to damage the district systems, or an component of the network; to strip or harvest information, to completely take over a person's computer, or to allow the intruder to "look around." Any user who violates this prohibition will be strictly liable for any damage to district systems without regard to intent to cause harm. The act taken in violation of this policy shall be sufficient to establish the individual's intent to cause harm.

2. Altering or attempting to alter files, system security software, computing or networking components (including but not limed to fileservers, bridges, routers or hubs), or any district system without authorization.

3. Unauthorized scanning of the district systems for security vulnerabilities.

4. 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, or by any other means.

5. Connecting unauthorized hardware and devices to the network and district systems.

6. Damaging the district systems or networking equipment through the user's negligence or deliberate act, including acts taken for purposes other than causing harm which are in violation of this policy.

7. Failing to comply with requests from appropriate teachers or district administrators to discontinue activities that threaten the operation or integrity of the district systems or networking equipment.

	Copyright
17 U.S.C. Sec. 101 et seq Pol. 814	The illegal use of copyrighted software by students and staff is prohibited. Any data uploaded to or downloaded from the network shall be subject to fair use guidelines. Federal laws, cases, and guidelines pertaining to copyright will govern the use of material accessed through the district resources. All users must comply with the mandates of copyright law and shall not use copyrighted materials illegally or without a proper license, nor shall any user commit an act of plagiarism. The illegal use of copyrighted materials is strictly prohibited. Employees will model proper respect for copyright laws and intellectual property and will instruct students to respect copyrights, request permission when appropriate, and comply with license agreements. Violation of copyright law may be a felony and the law allows a court to hold individuals personally responsible for copyright infringement. The district does not, and will not, tolerate violations of federal copyright law. Therefore any user violating federal copyright law does so at their own risk and assumes all liability for their actions. Violations of copyright law include, but are not limited to, the making of unauthorized copies of any copyrighted material (such as commercial software, graphic images, audio and video recordings), distributing copyrighted materials over computer networks, and deep-linking and framing into the content of others' websites. Further, the illegal installation of copyrighted software or files for use on the district's computers is expressly prohibited. This includes all forms of licensed software – shrink wrap, click wrap, browse wrap, and electronic software downloaded from the internet. District guidelines regarding plagiarism will govern the use of material accessed through the district systems. Users will not plagiarize works that they find and actions of plagiarism are strictly prohibited and will be subject to appropriate punishment. Teachers will instruct students in appropriate research and citation practices.

Other Electronic Communications Notices

Other electronic communications include but are not limited to e-mail, chat rooms, discussion boards, blogging, twitter, instant messages, journaling, or any other communication tool.

1. Electronic communication is subject to district review at any time. No electronic communication sent through the district system is private. Under certain circumstances, such as a result of investigations, subpoenas, lawsuits, or other legally sufficient requests, the district may be required by law to disclose the contents of e-mail communications.

2. Access to e-mail programs or web-based e-mail providers, other than the approved district e-mail program, is prohibited on the network. All school-related correspondence must be sent via the e-mail account provided by the district.

3. Other types of communication programs are to be used for educational purposes only and must be connected to the curriculum. All communication programs which the faculty wishes to use for educational purposes must be reviewed and approved by the Superintendent or his/her designee.

Search And Seizure

Violations of this policy, any other district policy, or the law may be discovered by routine maintenance and monitoring of the district systems or by any method stated in this policy or pursuant to any other legal means.

The district reserves the right to monitor, track, log, and access any electronic communications, including but not limited to, internet access and e-mails, at any time for any reason. Users have no expectation of privacy in their use of the district systems and technology, even when used for incidental personal reasons. Further, the district reserves the right, but not the obligation, to access any personal technology device of users brought onto the district's premises or at district events, or connected to the district network, containing district programs, data, or student data, in order to ensure compliance with this policy and other district policies, to protect the district's systems, and to comply with all applicable laws.

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

Security

Lewisburg Area School District has several safeguards in place to protect students from accessing information that is not suited for educational purposes. Network 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 the greatest extent possible, internet filtering software is in place to monitor and block inappropriate material from access by students and staff. The Superintendent or designee may authorize the disabling of filtering software during use by an adult to enable access for bona fide research or other lawful purposes. To protect the integrity of the network, the following procedures shall be followed:

1. Employees and students shall not reveal their passwords to another individual.

2. Users may be required to change their passwords at any time and should change their passwords regularly.

3. Users are not to use a computer that has been logged in under another student's or employee's name.

4. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the network.

Consequences For Inappropriate, Unauthorized And Illegal Use

General rules for behavior, ethics, and communications apply when using the district computer equipment, network and information, in addition to the stipulations of this policy, other district policies, rules, and procedures, Internet Service Provider terms, and local, state, and federal laws. Users must be aware that violations of this policy or other district policies, rules, and procedures or for unlawful use of the network, may result in loss of district access and a variety of other disciplinary actions, including, but not limited to, warnings, usage restrictions, loss of privileges, oral or written reprimands, student suspensions, employee suspensions (with or without pay), dismissals, expulsions, and/or legal proceedings on a case-by-case basis.

24 P.S. Sec. 4604	The user is responsible for damages to the equipment, network, electronic communications systems, and software resulting from negligent, deliberate or willful acts. The user will also be responsible for incidental or unintended damage resulting from negligent, deliberate or willful violations of this policy. Users shall be responsible for payments related to lost or stolen computers and any other electronic equipment, and recovery and/or breach of data contained on them. 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. **Vandalism** is any malicious attempt to harm or destroy the district's computers, data, applications, and/or network functionality or the data, applications, or functionality of another user's computer. This includes but is not limited to the uploading or creation of computer viruses. Vandalism may result in cancellation of access privileges and is subject to discipline. Any and all costs incurred by the district for repairs and/or replacement of software, hardware, data files and for technological consultant services due to any violation of this policy, other district policies, rules, and procedures, or Internet Service Provider, local, state or federal law must be paid by the user who causes the loss. The cost will be determined on a case-by-case basis. Users should be aware that under Pennsylvania law it is a crime to access, alter, or damage any computer system, network, software, or database, or any part thereof, with the intent to interrupt the normal functioning of an organization. It is also unlawful to knowingly and without authorization disclose a password to any computer system or network, to gain unauthorized access to a computer or to interfere with the operation of a computer, or to alter any computer software without authorization. Violations of these sections of Pennsylvania law are a felony punishable by a fine of up to $15,000 and up to seven (7) years of imprisonment. Disclosure of a password to a computer system or network knowingly and without authorization is a misdemeanor punishable by a fine up to $10,000 and imprisonment of up to five (5) years. Users are placed on notice that their actions in violation of this policy and the law, as described herein, can and will, where appropriate, result in criminal and/or civil prosecution.

	Safety The LASD wants network and equipment users, to the greatest extent possible, to be protected from harassment, bullying or unwanted or unsolicited communication. Any network user who receives threatening, harassing or unwelcome communications shall immediately bring them to the attention of a teacher or administrator. Network users shall not reveal personal information to other users on the network, including chat rooms, e-mail, Internet, etc.
20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254	Any district computer/server utilized by students and staff shall be equipped with Internet blocking/filtering software. Parents/Guardians with questions relating to the network and its use by their children should contact the appropriate building administrator.
47 U.S.C. Sec. 254 47 CFR Sec. 54.520	Internet safety measures shall address the following: 1. Control of access by minors to inappropriate material 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 minor's access to materials deemed harmful to them. Along with the use of this resource come certain responsibilities. Even though all training in the use of the district's telecommunications network will emphasize the ethical use of this resource, it is possible that a student, employee, or guest may come across some material that they or a parent/guardian may find objectionable. While the district will take reasonable steps to preclude access to such material through electronic filtering and classroom management, it is not possible for the district to guarantee that it can completely prevent access to objectionable materials.

Student Photos On District Website

The district website is intended to be a source of information for the entire school community, including all school staff, parents/guardians, and students. As part of the initiative to relay as much information as possible to the community, it may be necessary to publish photographs and student projects on the website. Students shown in photographs that are published on the website will not be identified. Captions may identify some photographs, but these captions will not include student names.

Definitions

18 U.S.C. Sec. 2256

Child Pornography - any visual/audible 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/audible depiction involves the use of a minor engaging in sexually explicit conduct.

2. Such visual/audible depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

3. Such visual/audible 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.

Computer - includes but is not limited to desktops, notebooks, powerbooks, tablet PCs, laptops, printers, cables, modems, other peripherals, specialized electronic equipment used for students' special educational purposes, global positioning system equipment, personal digital assistance, cell phones, mobile phones, other wireless devices, beepers, paging devices, two-way radios/telephones, laser pointers and attachments, and any other such technology developed.

20 U.S.C. Sec. 6777
47 U.S.C. Sec. 254

Harmful to Minors - any picture, image, graphic image file, or other visual/audible depiction that:

1. Taken as a whole, with respect to minors, appeals to the prurient interest in nudity and sex.

	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, or scientific value as to minors. **Incidental Personal Use** - use by an individual employee for occasional personal communications. Under no circumstances should the user assume that incidental personal use is private.
18 Pa. C.S.A. Sec. 5903	**Obscene** - material will be considered obscene when it 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, or scientific value. **User** - any student, staff, employee, faculty member, or guest who accesses any district network resources or facilities, including but not limited to, district computers, the district network, district hardware, district software, accesses the Internet through the district's connection, or through any other district systems.

	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, 218, 218.2, 220, 233, 237, 248, 249, 317, 348, 814