LOYALSOCK TOWNSHIP SCHOOL DISTRICT

SECTION: OPERATIONS

TITLE: ACCEPTABLE USE OF INTERNET, NETWORKS AND TECHNOLOGY RESOURCES

ADOPTED: February 12, 1997
REVISED: November 5, 2008
December 8, 2010
April 20, 2011
April 11, 2012

815. ACCEPTABLE USE OF INTERNET, NETWORKS AND TECHNOLOGY RESOURCES

1. Purpose

The Board supports use of the Internet, networks, and technology resources in the district's instructional and operational programs in order to facilitate learning, teaching and daily operations. The Acceptable Use Policy provides the terms and conditions that must be accepted by students, parents and legal guardians, staff, guests, and affiliated agencies regarding the acceptable use, rules of behavior, and access privileges to the Internet, email correspondence, the use of computer hardware and peripherals, and the installation and maintenance of software.

For instructional purposes, the use of the Internet, networks, and technology resources shall be consistent with the curriculum adopted by the school district as well as the varied instructional needs, learning styles, abilities, and developmental levels of students as well as the operational needs of the school district.

The Internet and the World Wide Web is a vast information network that links individuals, computers, networks, and databases throughout the world. The Internet has the potential to serve as an invaluable resource because it allows immediate access to and download of educational materials. All users must be aware that the Internet's power to access limitless information resources also includes information or materials that lack educational value and can be inaccurate, controversial, objectionable, offensive, defamatory, and even illegal. The Loyalsock Township School District does not condone the use of the district technology resources for these purposes. However, it is technologically impossible for the district to adequately filter or control the quality or content of the information available on the Internet while still retaining a meaningful connection to it. Therefore, all users will be held responsible for ensuring their activities adhere to the district's Acceptable Use Policy and to generally accepted educational standards as outlined in other applicable district policies, whether the district equipment is used at the workplace, conference, residence, or other locations.

	The Internet also provides new and exciting interactive communication technologies such as podcasts, blogs, wikis, and discussion groups. While these interactive technologies hold great educational potential for learning, they can also be disruptive if improperly utilized. Use of these interactive technologies must be related to district business or have an educational purpose. Users should understand that there is a distinct lack of confidentiality on the Internet. The email system is for business use only and prohibits any business unrelated to district matters. It is recognized, however, that employees may use their email for incidental personal use, but there is no expectation of privacy in such use. Incidental personal use is that use which is occasional, infrequent use which does not impact an employee's duties, does not impact network resources, and does not impede educational operations. This Board supports and promotes positive and effective digital citizenship among all district users.
2. Authority	The electronic information available to students and staff does not imply endorsement by the district of the content, nor does the district guarantee the accuracy of information received. The district shall not be responsible for 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 shall not be responsible for any unauthorized charges or fees resulting from access to the Internet. The district reserves the right to log network use and to monitor fileserver space utilization by district users, while respecting the privacy rights of both district users and outside users. The Board establishes that network use is a privilege, not a right; inappropriate, unauthorized and illegal use will result in cancellation of those privileges and appropriate disciplinary action. The district's technology system administrators and staff have access rights to user accounts to conduct normal and routine business and security functions regarding technology integration and technical support for the users of the district. The district shall make every effort to ensure that this resource is used responsibly by students and staff.

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 sources, 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 the district. The building administrator shall have the authority to determine what is inappropriate use. The Director of Technology or his/her designee will oversee the district's technology systems and will work with district, regional, or state organizations to educate employees and provide leadership for proper training in the use of the district's technology systems and requirements of this policy. The district's Director of Technology or his/her designee will maintain a procedure for creating and assigning individual accounts, set quotas for disk usage on the system, establish a data file retention schedule, maintain the school district virus protection process, monitoring network traffic, processor and system utilization, and all applications provided through the network and communication systems, including email. The Superintendent of Schools or his/her designee is responsible for ensuring the security of personal and confidential data maintained in employee or student information management systems. In systems not maintained by the district on district equipment, the Superintendent or his/her designee is responsible for periodic auditing to ensure that adequate security measures are in place. It is the express responsibility of all users to be aware of confidentiality rights governing such data and to protect the data.
4. Definitions	The term **technology resources** shall refer to any electronic device and instrument that uses, manages, carries, or supports audio, video, or data and includes, but is not limited to, information that is transmitted or received by radio, television, cable, microwave, telephone, computer systems, networks, and fax machines. The term **communication system** refers to the entire technological infrastructure and encompasses the collective use of the Internet, Intranet, email, coaxial and wireless telephone, pagers, facsimile machines, computer hardware and peripherals, duplication machines, audio and video recording machines, television,

CD/DVD/VCR recorders and players, still and motion picture cameras and projectors, digital environmental control systems, security and safety monitoring systems, and any other instrument or device used to transmit and receive electronic literary and/or audio and visual information.

The term **user** applies to students enrolled in grades K-12 as well as employees, substitutes, consultants, contractors, parents/guardians, guests, and all affiliated agents.

The Superintendent or designee shall be responsible for recommending technology and developing procedures used to determine whether the district's computers are being used in violation of this policy or 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 child pornography; crime; violence; intolerance; obscenity; profanity; rude and disrespectful language; inflammatory, threatening, or abusive, text, graphics, or video imagery; and any other items 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 for users.

3. Monitoring online activities of minors and adults as necessary. The district has the option to utilize random electronic surveillance when it is discovered that a user has and/or intends to install and/or access unauthorized software and/or software that is restricted by licensing to a single user at one workstation while being made accessible to multiple users at more than one workstation. Random electronic surveillance may also be used to detect when a user accesses prohibited websites.

4. Software installed on district-owned hardware must be licensed by the district, and the license and the purchase documentation must be on file with the district's Director of Technology. Users may not install personal software on district-owned hardware. Users may be required to provide proof of licensing if there is a question regarding software installation and when none exists or cannot be produced, the software will be deleted.

	5. The district will not use any surveillance methodology to gather personal identifying information (names, home addresses, etc.) about any of its users. However, users have no privacy expectations in the contents of their personal files and records or their online activity while using district technologies and the communication system.
5. Guidelines	Network accounts shall be used only by the authorized owner of the account for its approved purpose; access to a user's account is not to be shared with other users other than district technology system administrators and staff that may need to provide support in the conduct of routine business. Users do not own accounts on the district network, but they are granted the privilege of use. District system administrators are permitted access to user files in the normal course of their employment when necessary to conduct district business, to protect the integrity of communications systems and property of the district and may examine or make copies of files that are suspected of misuse or that have been corrupted or damaged, for example, or to provide routine technical support. Users accounts may be subject to search by law enforcement agencies pursuant to a court order. Misuse of the communication systems and technology resources or other information resources may result in the loss of computing accessibility, disciplinary actions as described in the penalties section, or can be prosecuted under applicable statutes. Employees' access to technologies and communication systems will cease immediately when the users' employment is terminated. Students' access to technologies and communications systems will cease immediately when the student users vacate the classroom environment because of expulsion, graduation, or relocation/transfer to another school system. Network users shall respect the privacy of other users on the system. The school district shall provide a copy of this policy to all district users in appropriate handbooks and posted on the district website. The school district encourages parents/guardians to review this policy and discuss with their child(ren) what material is and is not acceptable for their child(ren) to access in school through the district's technology resources.

Prohibitions

All users 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. Specifically, the following uses are prohibited:

1. Users are not to share their network password with others except with district technology staff who may need to access the user's account to provide technical support or conduct other business related to technology integration in the district.

2. Unauthorized use of a computer account, including trespassing in another user's folders, work, files, or emails.

3. Revealing personal information in violation of the district's confidentiality policy.

4. Using the district network to gain or attempt to gain authorized access to any computer system.

5. Misrepresenting the user's identity of the district in electronic correspondence.

6. Connecting unauthorized equipment to any part of the district network.

7. Unauthorized attempts to circumvent data protection schemes or uncover security loopholes and/or decrypt intentionally secure data.

8. Deliberately or carelessly performing an act that will interfere with the normal district operation of computers, terminals, peripherals, or network.

9. Deliberately or carelessly installing or running a program intended to damage or to place excessive burden on a district computer system or network. This includes, but is not limited to, programs known as computer viruses, Trojan horses, and worms.

10. Deliberately wasting or overloading computer resources, such as printing large quantities of a document from a workstation.

11. Violating terms of applicable software licensing agreements or copyright laws.

12. Violating copyright laws and their fair use provisions through inappropriate reproduction or dissemination of copyrighted text; images, audio, video, etc.

	13. Knowingly using electronic mail to harass or threaten others (includes sending repeated, unwanted mail to another user). 14. Initiating or propagating electronic chain letters. 15. Inappropriate mass mailing, which includes spamming, flooding, or bombing. 16. Forging the identity of a user or machine in an electronic communication. 17. Transmitting or reproducing materials that are slanderous or defamatory or that otherwise violate existing laws and regulations. 18. Displaying or downloading obscene, lewd, sexually harassing or otherwise materially offensive images, text, or audio. 19. Attempting to monitor or tamper with another's electronic communications or reading, copying, altering, or deleting another user's files or software without the explicit agreement of the owner. 20. Using the district network and/or technology resources to engage in any commercial, for-profit, or any business purpose (except where such activities are otherwise permitted or authorized under applicable school district policies). **Commercial purposes** are defined as offering goods or services or purchasing goods or services for personal use. 21. Engaging in unauthorized fundraising or advertising on behalf of the school district or nonschool district organizations. 22. Using the district network and/or technology resources to engage in activities that do not support learning, instruction, or operational/support processes. 23. Facilitating any type of illegal activity. 24. Using the network and/or technology resources for product advertisement or political lobbying.
SC 1303.1-A Pol. 249	25. Bullying/cyberbullying. 26. Using or distributing hate mail, discriminatory remarks, or inflammatory communication. 27. Quoting of personal communications in a public forum without the original author's prior consent.

28. Wasting bandwidth resources for online activities that serve no educational or operational purpose, such as playing noneducational games.

29. Revealing any personal information about any users on websites, blogs, podcasts, videos, wikis, email, or as content on any other electronic medium that is accessible to the general public and in violation of state and national laws concerning privacy.

30. Connecting nondistrict-owned personal computers or other Internet accessible devices on school district premises and property, at school district events through a connection to the school district technology systems, unless permission has been granted by the Director of Technology or his/her designee.

31. Installing nondistrict-owned computer hardware, peripheral devices, network hardware, or system hardware on the district network. The authority to install hardware and devices is restricted to the Director of Technology or his/her designee.

32. Scanning of the district's technology systems for security vulnerabilities without authorization.

33. Using routers or switches, or configuring wireless technology, attempting to create network connections, or extending any computer, telephonic device, electronic communications system, or network services, whether wired, wireless, cable, or by other means, without authorization.

34. Utilizing district technology resources to conduct denial of service attacks on district or other systems.

35. Accessing, interfering with, possessing, or distributing confidential or private information unless within the scope of the position's responsibility.

36. Encrypting messages using encryption software that is not authorized by the school district from any access point on school district equipment or school district property.

37. Other items not covered on this list will be addressed, as necessary, by the Superintendent or his/her designee.

	Acceptable Network Use Examples 1. Creation of files, projects, videos, web pages, and podcasts using network resources in support of educational and operational research, efficiency, and communication. 2. Participation in blogs, wikis, bulletin boards, social networking sites, and groups and the creation of content for podcasts, email, and web pages that support educational and operational research, efficiency, and communication. 3. The online publication of original educational material, curriculum-related materials, and student work that support educational and operational research, efficiency, and communication. 4. Staff use of the network for incidental personal use in accordance with all district policies and guidelines. Security 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. Users shall not reveal their passwords to another individual other than district system technology administrators to conduct normal and routine educational, operational, and technical support functions. 2. Users, other than district technology staff, are not to use a computer that has been logged in under another student's or employee's name without their knowledge. 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. 4. Users must notify the district's Director of Technology or his/her designee immediately if they have identified a possible security problem. Consequences For Inappropriate Use
24 P.S. Sec. 4604	The 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 communications apply when using the Internet, in addition to the stipulations of this policy. Loss of access and other disciplinary actions shall be consequences for inappropriate use.

Vandalism shall result in cancellation of access privileges. **Vandalism** is defined as any malicious attempt to harm or destroy data of another user, Internet or other networks; or damage of district technology resources. This includes, but is not limited to, uploading or creating computer viruses.

Penalties – All Users

Major infractions or repealed minor infractions of this Acceptable Use Policy (AUP) may result in penalties that include the temporary or permanent loss of the district communications system access or the modification of the user's access. More serious violations, such as the unauthorized use or duplication or licensed software, data files, passwords of other users, harassment or threatening behavior, will be subject to disciplinary action that may result in suspension or employment termination.

Any offense that violates local, state, or federal laws may result in the district contacting legal authorities and criminal charges being filed that may result in litigation, arrest, and imprisonment.

All allegations of AUP violations will be handled in accordance with employee discipline.

Level 1 Penalties –

General infractions that result in no loss of data or damage to a technology resource and are not classified as a misdemeanor or felony. This level includes account sharing and misuse of computer resources. Penalty may include suspension from access to technology resources, detention, reduction of a grade, removal from class, suspension, or a letter of reprimand.

	Level 2 Penalties – Infractions that result in minor loss of data or damage to a technology resource and are not classified as a misdemeanor or felony. This level includes unauthorized deletion of data files and unauthorized shutdown of file servers. Penalty may include suspension from access to technology resources, detention, loss of a grade, removal from class, suspension, a suspension from the workplace, and the recovery of costs to replace data or resources. ***Level 3 Penalties –*** Infractions that result in irreplaceable loss of data or severe damage to a technology resource and are classified as a misdemeanor or felony. This includes copyright violations and virus introduction into a computer or network. Penalty may be payment for recovery costs to replace data or resources, permanent suspension from technology resource access, expulsion, possible criminal charges, termination of employment, and possible litigation. In conducting all investigations and administrating penalties under this policy, the district will ensure that the rights of all district employees under state and federal laws and the applicable collective bargaining agreements shall be protected. <u>Copyright</u> The illegal use of copyrighted software by students and staff is prohibited. Downloading, copying, duplicating and distributing software, music, sound files, movies, images, or other copyrighted materials without the specific written permission of the copyright owner is generally prohibited. Any data uploaded to or downloaded from the network shall be subject to fair use guidelines of the United States Copyright law. <u>Safety</u> To the greatest extent possible, users of the network will be protected from harassment and unwanted or unsolicited communication. Any network user who receives threatening or unwelcome communications shall report such immediately to a teacher, administrator, or the Director of Technology.
17 U.S.C. Sec. 101 et seq Pol. 814	

All district computer/server users shall be equipped with Internet blocking/filtering software. Filtering software is not one hundred percent (100%) effective, and every user must take responsibility for his/her use of the network and Internet and avoid objectionable sites.

All students will receive instruction on Internet safety and appropriate Internet behavior compliant with the "Protecting Children in the 21st Century Act". The lessons will specifically include interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness along with an emphasis on Internet predators and reporting policies and procedures.

47 U.S.C.
Sec. 254
47 CFR
Sec. 54.520

Internet safety measures shall effectively address the following:

1. Control of access by minors to inappropriate matter on the Internet and World Wide Web.

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.

Exemptions

The district recognizes that the job requirements of several positions may conflict with the specific language of the policy. Accordingly, the Superintendent may exempt such positions from this policy as necessary to carry out their individual responsibilities. Among the positions recognized as entitled to an exemption are: Director of Technology, Network Administrator, and IT support staff.

Archive And Backup

Backup is made of all district email correspondence in accordance with district policy and other applicable state and federal statutes and for disaster recovery. Barring technical issues or power outages, all users' files are backed up on district severs nightly.

Limitations Of Liability

The school district makes no warranties of any kind, either expressed or implied, that the functions or services provided by or through the district's systems will be error-free or without defect.

The school district does not warrant the effectiveness of Internet filtering. The school district shall not be responsible for material that is retrieved through the Internet or the consequences that may result from them.

The school district shall not be responsible for any damages users may suffer, including but not limited to, information that may be lost, damaged, delayed, or unavailable when using the computers, network, and electronic communications systems.

In no event shall the school district be liable to the user for any damages whether direct, indirect, special or consequential, arising from the use of the 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, 103.1, 104, 218, 218.2, 220, 233, 237, 248, 249, 317, 348, 814