SECTION: OPERATIONS

TITLE: COMPUTER HARDWARE/ SOFTWARE/NETWORK USAGE

KUTZTOWN AREA SCHOOL DISTRICT

ADOPTED: November 18, 1996

REVISED: September 21, 1998
July 16, 2001
August 1, 2005
September 17, 2009

815. COMPUTER HARDWARE/SOFTWARE/NETWORK USAGE

1. Purpose

The Board supports use of computer hardware, software, Internet and other computer networks in the district's instructional and operational programs in order to facilitate learning, teaching, and daily operations through interpersonal communications and access to information, research and collaboration for employees, students and guests.

For instructional purposes, the use of computer hardware, software and network facilities shall be consistent with the district's mission, curriculum adopted by the district, as well as the varied instructional needs, learning styles, abilities, and developmental levels of students.

2. Authority

It is the Board's belief that all computer hardware acquired for or on behalf of the district shall be deemed district property and shall remain with the district upon the resignation, retirement, termination or other separation from employment of the employee.

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 is lost, damaged or unavailable when using hardware, software or 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.

47 U.S.C. Sec. 254

Access to the district's hardware, software, and network use is a privilege, not a right. These, as well as the user accounts and information, are the property of the district, which reserves the right to deny access to prevent further unauthorized, inappropriate or illegal activity, and may revoke those privileges and/or administer appropriate disciplinary action. The 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 network. The district shall establish a list of materials, in addition to those stated in law, that are inappropriate for access by minors.

	It is often necessary to access user accounts in order to perform routine maintenance and security tasks; system administrators have the right to access by interception, the stored communication of user accounts for any reason in order to uphold this policy and to maintain the network. Users have no privacy expectation in the contents of their personal files and any of their use of the district's network. The district reserves the right to monitor, track log and access the network's use and to monitor and allocate fileserver space.
20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254	The 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. The district operates and enforces technology protection measures that block or filter online activities of minors on computers used and accessible to adults and students so as to filter or lock inappropriate matter on the Internet. Inappropriate matter includes, but is not limited to, visual, graphic, text and any other form of obscene; sexually explicit; child pornographic; or other material that is harmful to minors; 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; terroristic; and advocates destruction of property. Measures designed to restrict adults' and minors' access to material harmful to minors may be disabled to enable an adult or student 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. 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. 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 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	The Director of Information Technology and/or designee will serve as the coordinator to oversee the district's network and will work with other organizations as necessary to educate users, approve activities, provide leadership for proper training for all users in the use of the network resources and the requirements of this policy, establish a system to ensure adequate supervision of the network, maintain executed user agreements, and interpret and enforce this policy. Due to the nature of the Internet as a global network connecting thousands of computers around the world, inappropriate materials, including those which may be defamatory; discriminatory as it pertains to race, color, religion, national origin, gender, marital status, age, sexual orientation, political beliefs, receipt of financial aid, or disability; inaccurate; obscene; sexually explicit; lewd; vulgar; rude; harassing; violent; inflammatory; threatening; terroristic; hateful; bullying; profane; pornographic; offensive; or illegal, 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 access to these resources. Accessing these and similar types of resources may be considered an unacceptable use of school resources and will result in consequences detailed in this and other relevant district policies. The district shall make every effort to ensure that hardware, software and network resources are used responsibly by students and staff. Users must be capable and able to use the district's network, and software relevant to their responsibilities. In addition, users must practice proper etiquette, district ethics, and agree to the requirements of this policy. 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. All users have the responsibility to respect the rights of all other users within the district and to abide by the rules established by the district, local, state and federal laws. The Director of Information Technology and/or designee shall establish a process for

	setting-up individual and class accounts, set quotas for disk usage on the network, establish a document retention and destruction policy, and schedule to include electronically stored information, and establish the school district virus protection process.
4. Guidelines	<u>Access To The Network</u> Network user accounts will be used only by the authorized owner of the account for its approved purpose. An account will be made available according to a procedure developed by appropriate district authorities. Each employee 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 employee's place of residence, or in any other location such as a hotel, conference room, car or airport. Where possible, employees must avoid leaving their laptop unattended in an automobile. If they must do so temporarily, the laptop shall be placed out of view. Employees shall be responsible for all content on their district issued laptop. All district computer and laptop content may be monitored by the district. Employees are not permitted to install software or alter the operating system without the permission of the technology department. <u>School District Limitation Of Liability</u> The district makes no warranties of any kind, either expressed or implied, that the functions or the services provided by its network 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 network. The district shall not be responsible for any damage users may suffer, including but not limited to, information that may be lost, damaged, delayed, or unavailable when using the computers, network, and electronic communication system. <u>Prohibitions</u> 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. Specifically, the following uses are prohibited:

SC 1303.1-A Pol. 249	1. Facilitating illegal activity. 2. Commercial or for-profit purposes. 3. Nonwork or nonschool related work. 4. Product advertisement or political lobbying. 5. Bullying/Cyberbullying. 6. Hate mail, discriminatory remarks, and harassing, offensive or inflammatory communication. 7. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials. 8. Access to obscene or pornographic material or child pornography. 9. Access by students and minors to material that is harmful to minors or is determined inappropriate for minors in accordance with Board policy. 10. Inappropriate language or profanity. 11. Transmission of material likely to be offensive or objectionable to recipients. 12. Intentional obtaining or modifying of files, passwords, and data belonging to other users. 13. Impersonation of another user, anonymity, and pseudonyms. 14. Fraudulent copying, communications, or modifications of materials in violation of copyright laws. 15. Loading or using of unauthorized games, programs, files, or other electronic media. 16. Disruption of the work of other users. 17. Destruction, modification, abuse or unauthorized access to network hardware, software and files. 18. Quoting of personal communications in a public forum without the original author's prior consent. 19. Participation in unauthorized Internet relay chats, instant messaging, and Internet

voice communications that are not for school-related purposes or required for employees to perform their job duties.

20. Install, distribute, reproduce or use copyrighted software on district computers, or copy district software to unauthorized computer systems, intentionally infringing upon the intellectual property rights of others or violating a copyright.

21. 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.

22. Send unsolicited commercial e-mail messages, also known as spam.

Software

All users shall be responsible to take precautions to prevent the introduction of viruses to district-owned equipment. Attempts to degrade or disrupt any district-owned computer or network system performance by spreading computer viruses is considered criminal activity under state and federal law.

The unauthorized installation or downloading of software or files for use on district-owned computers is prohibited. Software may not be installed on any district-owned computer without the written permission of the Director of Information Technology.

Users of district-owned software shall abide by the software licensing agreement provided by the software publisher. Software piracy, the illegal use or possession of copyrighted software, is strictly prohibited.

E-mail

E-mail may not be used for private purposes or commercial offerings of products or services for sale or to solicit products or services.

E-mail may not be used for political or religious purposes.

E-mail messages are subject to district staff review at any time.

E-mail may not be used to broadcast messages outside a school-owned building.

Students are not permitted to use e-mail unless given written permission by a district administrator.

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. Employees and students shall not reveal their accounts or passwords to another individual. Users may not share their account with anyone or leave their account open or unattended. Violations traced to an individual account name will be treated as the sole responsibility of the owner of the account.

2. Users are not to use a computer that has been logged in under another student 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.

4. Users are not to use district resources to engage in any illegal act, which may threaten the health, safety or welfare of any person or persons; such as, engaging in criminal activity, or being involved in a threat against any person or property.

Users must immediately notify the Director of Information Technology and/or designee if they have identified a possible security problem.

Operational Prohibitions

The following operational activities and behaviors are prohibited:

1. Interference with or disruption of the network, network accounts, services or equipment of others, including, but not limited to, the propagation of computer worms and viruses, the sending of electronic chain mail, distasteful jokes, and the inappropriate sending of "broadcast" messages to large numbers of individuals.

2. Connecting unauthorized hardware and devices to the district network.

3. Intentionally destroying the district's computer hardware or software.

4. Intentionally disrupting the use of the district's network.

5. Damaging the district's network, networking equipment through the users' negligence or deliberate act.

Safety

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 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.
47 U.S.C. Sec. 254	Internet safety measures shall effectively 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>Content Guidelines</u> Information electronically published on the district's network shall be subject to the following guidelines: 1. Published documents including, but not limited to, audio and video clips may not include a student's date of birth, Social Security number, driver's license number, health information, phone number, 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.
Pol. 814	4. Documents, web pages, and electronic communications, must conform to all district policies and guidelines, including the district's Copyright Policy.

5. Documents to be published on the Internet must be edited and approved according to district procedures before publication.

Copyright Infringement And Plagiarism

The illegal use or possession 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's resources. Users will make a standard practice of requesting permission from the holder of the work and complying with license agreements. Employees will instruct users to respect copyright, request permission when appropriate, and comply with 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 district does not permit illegal acts pertaining to the copyright law. Therefore, any user violating the copyright law does so at their own risk and assumes all liability. Violations of copyright law include, but are not limited to, the 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; 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 district's computers is expressly prohibited. This includes all forms of licensed software such as shrink wrap, clickwrap, browsewrap, and electronic software downloaded from the Internet.

District guidelines on plagiarism will govern use of material accessed through the district's network. Users will not plagiarize works that they find. Teachers will instruct students in appropriate research and citation practices.

Selection Of Material

When using the Internet for class activities, teachers will select material that is appropriate in light of the age of the students and that is relevant to the course objectives. Teachers shall 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 shall provide guidelines and lists of resources to assist their students in channeling their research activities effectively and properly. Teachers shall assist their students in developing the critical thinking skills necessary to ascertain the truthfulness of information, and distinguish fact from opinion.

School District Web Site

The district will establish and maintain a Web Site and will develop and modify its Web pages that will present information about the district under the direction of the Director of Information Technology and/or designee. Publishers must comply with this and other district policies.

Consequences For Inappropriate, Unauthorized And Illegal Use

The user is responsible for damages to the equipment, network, electronic communications systems, and software resulting from negligent, deliberate or willful acts. The user shall also be responsible for incidental or unintended damage resulting from 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/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.

General rules for behavior, ethics, and communications apply when using the Internet and the district network, in addition to the stipulations of this policy. Loss of access and other disciplinary actions shall be consequences for inappropriate use.

Vandalism will 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; this includes, but is not limited to, uploading or creating computer viruses.

References:

School Code – 24 P.S. Sec. 1303.1-A

Child Internet Protection Act – 24 P.S. Sec. 4601 et seq.

Enhancing Education Through Technology Act of 2001 – 20 U.S.C. Sec. 6777

Internet Safety – 47 U.S.C. Sec. 254

Board Policy – 249