East Penn School District

Acceptable Use Policy

Acceptable Use of Technology Resources, Electronic Communications and Information Systems
No. 815

Book	Policy Manual
Section	800 Operations
Title	Acceptable Use of Technology Resources, Electronic Communication and Information Systems
Number	815
Status	Active
Legal	1. 18 U.S.C. 2256 2. 18 Pa. C.S.A. 6312 3. 20 U.S.C. 6777 4. 47 U.S.C. 254 5. 18 Pa. C.S.A. 5903 6. Pol. 218 7. Pol. 233 8. Pol. 317 9. Pol. 103 10. Pol. 103.1 11. Pol. 104 12. Pol. 248 13. Pol. 348 14. Pol. 249 15. Pol. 218.2 16. 24 P.S. 4604 17. 24 P.S. 4610 18. 47 CFR 54.520 19. 24 P.S. 1303.1-A 20. Pol. 237 21. Pol. 814 22. 17 U.S.C. 101 et seq 23. Pol. 226 24. Pol. 824 25. Pol. 830 24 P.S. 4601 et seq Pol. 220
Adopted	September 11, 2017

Purpose

The Board supports the use of technology, information systems and the Internet 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.

The district provides students, staff and other authorized individuals with access to the district's computers, electronic communication systems and network, which includes Intranet/Internet access, whether wired or wireless, or by any other means.

The use of the district's technology resources must be consistent with the educational and administrative objectives of the school district.

Definitions

The term child pornography is defined under both federal and state law.

Child pornography - under federal law, is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where:[1]

1. The production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;

2. Such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or

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

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.[2]

The term harmful to minors is defined under both federal and state law.

Harmful to minors - under federal law, is any picture, image, graphic image file or other visual depiction that:[3][4]

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.

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:[5]

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.

Obscene - any material or performance, if:[5]

1. The average person applying contemporary community standards would find 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.

Technology protection measure - a specific technology that blocks or filters Internet access to visual depictions that are obscene, child pornography or harmful to minors.[4]

Authority

Access to the district's computing facilities, network, electronic communications, informational systems and other technology resources is a privilege, not a right. The district's technology resources, user accounts and information 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 Intranet/Internet, computers or network or technology resources, including personal files or any use of the district's Intranet/Internet, websites, computers or network or technology resources. The district reserves the right to monitor, track, and log network access and use; monitor fileserver space, processor and system utilization by district users; maintain email and fileserver quotas; or deny access to prevent unauthorized, inappropriate or illegal activity or use 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 technology systems.[6][7][8]

Employee and student use of personal technology devices brought onto school property that are connected to the district's network or contain district or student data or district-procured software programs shall comply with this policy and other applicable Board policies to protect the district's resources and to comply with law. Users may not use their personal technology devices to access the district's Intranet, Internet or any other technology resources unless approved by the Superintendent or designee. The district intends to strictly protect its technology systems against outside and internal risks and vulnerabilities.[6][8][20][23][24]

The Board requires all technology users to fully comply with this policy and to immediately report any violations or suspicious activities to the Superintendent or designee.

The Board establishes the following materials which, taken as a whole, lack serious literary, artistic, political, educational or scientific value, in addition to those stated in law and defined in this policy, that are inappropriate for access by minors:[4]

1. Defamatory.

2. Lewd, vulgar, profane, or sexually explicit.

3. Threatening.

4. Harassing or discriminatory.[9][10][11][12][13]

5. Bullying.[14]

6. Terroristic.[15]

The district reserves the right to restrict access to any Intranet/Internet sites or functions it deems inappropriate through established Board policy, or the use of software and/or online server blocking. Specifically, the district operates and enforces a technology protection measure(s) that blocks or filters access to inappropriate matter by minors on its computers used and accessible to adults and students. The technology protection measure shall be enforced during use of computers with Intranet/Internet access.[3][4][16]

Upon request by students or staff, the Superintendent or designee shall expedite a review and may authorize the disabling of Intranet/Internet blocking/filtering software to enable access to material that is blocked through technology protection measures but is not prohibited by this policy.[16]

Upon request by students or staff, building administrators may authorize the temporary disabling of Intranet/Internet blocking/filtering software to enable access for bona fide research or for other lawful purposes. Written permission from the parent/guardian is required prior to disabling Intranet/Internet blocking/filtering software for a student's use. If a request for temporary disabling of Intranet/Internet blocking/filtering software is denied, the requesting student or staff member may appeal the denial to the Superintendent or designee for expedited review.[3][17]

Delegation of Responsibility

The district shall make every effort to ensure that the district's technology resources, electronic communication, and information systems are used responsibly by technology users.

The district shall inform staff, students, parents/guardians and other users about this policy through employee and student handbooks, posting on the district website, and by other appropriate methods. A copy of this policy shall be provided to parents/guardians, upon written request.[16]

Users of district networks or district-owned equipment shall, prior to being given access to the district's network or being issued equipment, sign user agreements acknowledging awareness of the provisions of this policy, and awareness that the district uses monitoring systems to monitor and detect inappropriate use.

Student user agreements shall also be signed by a parent/guardian.

The Superintendent or designee shall be responsible for recommending technology and developing procedures used to determine whether the district's computers are being used for purposes prohibited by law or for accessing sexually explicit materials. The procedures shall include but not be limited to: [3][4][18]

1. Utilizing a technology protection measure that blocks or filters Intranet/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.

The Superintendent or designee shall develop and implement administrative regulations that ensure students are educated on network etiquette and other appropriate online behavior, including:[4]

1. Interaction with other individuals on social networking websites and in chat rooms.

2. Cyberbullying awareness and response.[14][19]

The Superintendent or designee shall be responsible for ensuring the security of personal and confidential data maintained in employee or student information management systems in accordance with Board policy.[25]

The Director of Technology or designee shall serve as the coordinator to oversee the district's technology systems and will work with district, regional or state organizations to educate employees, approve activities, provide leadership for proper training in the use of the systems and the requirements of this policy, establish a system to ensure adequate supervision of the technology systems, maintain executed user agreements, and interpret and enforce this policy.

The Director of Technology or designee shall maintain procedures for creating and assigning individual and class accounts, set quotas for disk usage on the system, establish a data file retention schedule, and maintain the school district virus protection process.

Guidelines

All users are expected to adhere to the requirements of this policy. All users are responsible for respecting the rights of other users within the district and district technology systems, to abide by the rules published by the district and its Internet Service Provider (ISP) and to obey local, state and federal laws.

Limitation of Liability

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

The electronic information available to users does not imply endorsement of the content by the district. The district shall not be responsible for material that is retrieved through the Internet or the consequences that may result from them.

The district is neither responsible for nor guarantees the accuracy or quality of the information obtained when using the district's systems.

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 district's computers, network and electronic communications systems.

The district shall not be responsible for any unauthorized financial obligations, charges or fees resulting from access to the district's systems. In no event shall the district be liable to the user for any damages whether direct, indirect, special or consequential, arising from the use of the district's systems.

Safety

It is the district's goal to protect users of the network from harassment and unwanted or unsolicited electronic communications. Any network user who receives threatening or unwelcome electronic communications or inadvertently visits or accesses an inappropriate site shall report such immediately to an administrator. Network users shall not reveal personal information to other users on the network, including chat rooms, email, social networking websites, etc.

Intranet/Internet safety measures shall effectively address the following:[4][18]

1. Control of access by minors to inappropriate matter on the Intranet/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 Intranet/Internet 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.

Prohibitions

The use of the district's technology resources, electronic communication and information systems for illegal, inappropriate or unacceptable purposes as designated by this policy is prohibited. Specifically, all users are prohibited from using these school systems to:

1. Send, receive, view, download, access, or transmit inappropriate matter and material likely to be offensive or objectionable to recipients including, but not limited to, that which may be defamatory, obscene, sexually explicit, lewd, hateful, harassing, discriminatory, violent, vulgar, rude, inflammatory, threatening, profane, pornographic, terroristic and/or illegal.

2. Bully/Cyberbully.[14][19]

3. Gamble.

4. Participate in discussion or news groups that cover inappropriate and/or objectionable topics or materials.

5. Participate in unauthorized Internet Relay Chats, instant messaging communications and Internet voice communications (online, real-time conversations).

6. Facilitate any illegal activity.

7. Mass mail noneducational or nonwork-related information (for example: the use of the "everyone" distribution list, building level distribution lists, or other email distribution lists to offer personal items for sale).

8. Engage in commercial, for-profit, or any business purposes (except where such activities are otherwise permitted or authorized under applicable Board policies) or conduct unauthorized fundraising or advertising on behalf of the district or nonschool district organizations.

9. Political lobbying for the purpose of electing public officials.

10. Install, distribute, reproduce or use copyrighted software not licensed by the district 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]

11. Install computer hardware, peripheral devices, network hardware or system hardware.

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

13. Access, interfere with, possess, or distribute confidential or private information unless within the scope of the position's responsibility.

14. Use the district's technology resources, electronic communication and information systems to send 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.

15. Post personal or professional web pages without administrative approval.

16. Post or transmit anonymous messages.

17. Utilize district equipment for conducting denial of service attacks on the district or other systems.

Access and Security

Users must immediately notify an administrator if they have identified a possible security problem or inadvertently accessed inappropriate material. The following activities related to access to the district's technology systems and information are prohibited:

1. Misrepresentation (including forgery) of the identity of a sender or source of communication.

2. Acquiring or attempting to acquire passwords of another user.

3. Altering a communication originally received from another person or computer with the intent to deceive.

4. Disabling, circumventing or attempting to defeat any district security measure, program or device, including, but not limited to, anti-spyware, anti-spam, and virus protection software or procedures.

Operational Prohibitions

The following operational activities and behaviors are prohibited:

1. Interfering with or disrupting, or attempting to interfere or disrupt the technology systems, network accounts, services or equipment of the district or others, including, but not limited to, the propagation of computer worms and viruses, Trojan Horse and trapdoor program code, and the sending of electronic chain mail. The user may not hack or crack, or attempt to hack or crack, the district's computing or networking components (including, but not limited to fileservers, bridges, routers, or hubs) or others' computers, whether by hardware, software, parasiteware, viruses and worms or other hardware or software designed to obtain information or damage the technology systems or any component of the network, and may not strip or harvest information, or take control of any computer without permission.

2. Altering or attempting to alter other users' or system files, system security software or the systems themselves, except for Information Technology staff in the performance of their duties.

3. Scanning of the technology systems for security vulnerabilities without authorization.

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

5. Failing to comply with requests from teachers or district administrators to discontinue activities that the teachers or administrators believe threaten the operation or integrity of the district's technology resources, electronic communication, and information systems.

Copyright Infringement and Plagiarism

Federal laws, cases and guidelines pertaining to copyright will govern the use of material accessed through district resources. Employees will instruct students to respect copyrights, request permission when appropriate, and comply with license agreements.[21][22]

District Website

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 and established administrative regulations.

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.

Consequences for Inappropriate, Unauthorized and/or Illegal Use

The user shall be responsible for damages to the network, equipment, systems, and software resulting from deliberate or willful acts.[16]

Illegal use of the network; intentional deletion or damage to files or data belonging to others; copyright violations; and theft of services shall be reported to law enforcement authorities for possible prosecution.

General rules for behavior and communications apply when using the Intranet/Internet, in addition to the stipulations of this policy.

Vandalism shall 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 (including non-district users); this includes but is not limited to uploading or creating computer viruses.

Violations of this policy or inappropriate or unlawful use of the technology systems may result in loss of technology access, disciplinary actions, up to and including termination, position reassignment, and/or legal proceedings on a case-by-case basis.[6][7][8]

EAST PENN SCHOOL DISTRICT

ACCEPTABLE USE POLICY AND INTERNET ACCESS ACKNOWLEDGEMENT FORM

I have read the East Penn School District Acceptable Use of Technology Resources, Electronic Communications and Information Systems Policy Brief and I will comply with its terms. The Acceptable Use of Technology Resources, Electronic Communications and Information Systems Policy #815 is available in the main office of each school and online. Go to http://www.eastpennsd.org. Scroll to the bottom of the homepage and select the Acceptable Use Policy link.

I understand that district technology resources are provided for the purpose of exploring educational topics, conducting research and classroom activities, and communicating with others in support of educational goals and the business of the district.

I understand that the district has the right to review any material stored on any system that the district provides and to edit or remove any material. I acknowledge that my access to such material is a privilege, not a right. I acknowledge that it is impossible for the district to restrict access to all controversial and inappropriate materials, and I will not hold the district responsible for the materials acquired on the network.

I understand that violation of this policy may have consequences ranging from revocation of access privileges to district disciplinary actions, and that violations may be reported to local, state, and/or federal legal authorities when applicable.

Name of Student (please print): _____ Student ID: _____

Student's Signature: _____

School: _____ Grade: _____ Date: ____/____ /_____

Name of Teacher: _____ (elementary only)

If above signatory is a minor, a parent or guardian signature is required. By signing below, I (as a parent or guardian) have read the above-mentioned policy and agree that my child and I will comply with its terms. I hereby give permission for my child to access the Internet as an academic resource.

Name (please print): _____

Signature of parent/guardian: _____ Date: ____/____ /_____

Phone: _____

Please sign this form and return it to your child's homeroom teacher by September 8, 2017. Forms will be kept on file in the main office.

EPSD Revised: 10/2017