Book
Policy Manual

Section
800 Operations

Title
Acceptable Use of Internet, Computers and Network Resources

Number
815

Status
Adopted 6/20/2016

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
24 P.S. 4601 et seq
Pol. 220

Purpose

The Board supports use of the computers, Internet and other network resources 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 Board promotes responsible, ethical, and legal utilization of technology by all users.

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

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

This policy does not attempt to describe every possible prohibited activity or misuse of technology by students with school staff. With technology constantly evolving, students and staff may have to make judgments about whether particular uses constitute a misuse of the network. All users are encouraged to seek guidance from a building administrator if they are uncertain about a particular use. Misuse generally falls under one of the following categories: using the network or device to access or communicate inappropriate materials, participate in illegal activities, violate copyright or software licenses, downloading apps or data from questionable sources, plagiarism, use for non-school purposes, misuse of passwords or unauthorized access, and malicious use or vandalism.

The district utilizes technology protection measures to restrict access to visual depictions that are obscene, child pornography, and/or harmful to minors. Deliberate use by students or staff of techniques, tools, or proxies to circumvent these measures is a violation of the acceptable use policy.

Authority

The availability of access to electronic information 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 or other network resources.

The Board declares that computer and network use is a privilege, not a right. The district's computer and network resources are the property of the district. Within reason, the board respects freedom of speech and access to information. The district may monitor usage connectivity to fix an issue, or investigate a complaint. Users should be aware that the district may review files and other communications to maintain the integrity of the network and to ensure everyone is using their district devices and network responsibly.[6][7][8]

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

The Board establishes the following categories of electronic content, in addition to those stated in law and defined in this policy, may be inappropriate for access by minors:[4]

1. Defamatory.
2. Lewd, vulgar, or profane.
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 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 Internet access.[3][4][16]

Upon request by students or staff, the Superintendent or designee shall conduct a review and may authorize the disabling of 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, technology administrators may authorize the temporary disabling of Internet blocking/filtering software to enable access for bona fide research or for other lawful purposes. If a request for temporary disabling of Internet blocking/filtering is denied, the requesting student or staff member may appeal the denial to the Superintendent or designee.[3][17]

Delegation of Responsibility

The district shall educate students in the responsible use of technology.

Administrators, teachers and staff have a professional responsibility to work together to help students develop the intellectual skills necessary to discern 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 will also be instructed 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]

Students, staff and other authorized individuals have the responsibility to respect and protect the rights of every other user in the district and on the Internet. The user to whom the account is assigned is the person allowed to use that account.

The district shall inform staff, students, families and other users about this policy through employee and student handbooks, posting on the district website, and by other appropriate methods. Access to this policy shall be provided to families [16]

Administrative regulations may be provided to assist students in understanding these guidelines (responsible use of technology) when requesting signatures for the AUP.

Users of district networks or district-owned equipment, software and apps prior to being given access or being issued equipment, shall sign user agreements acknowledging the provisions of this policy. The district reserves the right to use security systems to monitor, detect, and disable lost or stolen equipment accounts.

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

Administrators, teachers and staff have a professional responsibility to work together to help students develop the intellectual skills necessary to discern 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.

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 utilizing technology protection measures.[3][4][18]

Guidelines

Network accounts shall be used only by the authorized owner of the account for its approved purpose. Network users shall respect the privacy of other users on the system.

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 a teacher or administrator.

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

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.

Prohibitions

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. Commercial or for-profit purposes.
2. Product advertisement or political lobbying.
3. Impersonation of another user, anonymity, and pseudonyms.
4. Destruction, modification, abuse or unauthorized access to network hardware, software and files.
5. Accessing the Internet, district computers or other network resources without authorization.
6. Disabling or bypassing the Internet blocking/filtering software without authorization.
7. Accessing, sending, receiving, transferring, viewing, sharing or downloading confidential information without authorization.

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, these guidelines shall be followed:

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

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

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

Copyright

The illegal use of copyrighted materials is prohibited. Any data uploaded to or downloaded from the network shall be subject to fair use guidelines and applicable laws and regulations.[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.

Consequences for Inappropriate Use

The network user shall be responsible for damages to the 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 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.

Vandalism shall result in loss of access privileges, disciplinary action, and/or legal proceedings.

Failure to comply with this policy or inappropriate use of the Internet, district network or computers shall result in usage restrictions, loss of access privileges, disciplinary action, and/or legal proceedings.[6][7][8]

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]

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.

NOTES:

State CIPA – Child Internet Protection Act – 24 P.S. Sec. 4601 et seq.
Federal CIPA – Children's Internet Protection Act – 47 U.S.C. Sec. 254