Book	Policy Manual
Section	800 Operations
Title	Acceptable Use of Internet, Computers and Network Resources
Code	815
Status	Active
Adopted	August 10, 2010
Last Revised	November 1, 2016

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 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. This access has an educational purpose for students and is to facilitate employees' work productivity.

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.

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:[16]

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.[17]

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:[1][2]

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:[18]

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:[18]

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.[2]

Social Media - various forms of electronic communication to online communities.

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 has the right to place restrictions on the use of equipment, resources and material users access or disclose through the district's Internet, computers and network resources. Users are expected to follow the district's policies and administrative regulations governing conduct and discipline, and law and regulations, in their use of the district's Internet, computers and network resources. This access has not been established as a public access service or a public forum.

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. Users shall have no expectation of privacy in anything they create, store, send, receive or display on or over the district's Internet, computers or

network resources, including personal files or any use of the district's Internet, computers or network resources. The district reserves the right to monitor, track, and log network access and use; monitor fileserver space utilization by district users; or deny access to prevent unauthorized, inappropriate or illegal activity and may revoke access privileges and/or administer appropriate disciplinary action. The district shall cooperate to the extent legally required with the ISP, local, state and federal officials in any investigation concerning or related to the misuse of the district's Internet, computers and network resources.[3][4][20]

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 materials, in addition to those stated in law and defined in this policy, that are inappropriate for access by minors:[2]

1. Defamatory.
2. Lewd, vulgar, or profane.
3. Threatening.
4. Harassing or discriminatory.[5][6][21]
5. Bullying.[7]
6. Terroristic.[8]
7. Obscene.
8. Child pornography.
9. Harmful to minors.
10. Other materials prohibited by law or this policy, including but not limited to those deemed necessary upon recommendation of the Superintendent or designee.

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.[1][2][9]

Upon request by staff temporary 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 may be initiated.[9]

Staff may request authorization from the Director of Technology, or designee, to permanently disable Internet blocking/filtering software to enable access to material that is blocked through technology protection measures but is not prohibited by this policy. If a request for temporary or permanent disabling of Internet blocking/filtering software is denied, the requesting staff member may appeal the denial to the Superintendent or designee for expedited review.[1][10]

Delegation of Responsibility

The district shall make every effort to ensure that this resource is used responsibly by students and staff.

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.[9]

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

A parent/guardian can opt their student out of use of district internet, computers and/or network resources through an annual written request to the building level administrator.

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, 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.

Building administrators shall make initial determinations of whether inappropriate use has occurred.

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:[1][2][13]

1. Utilizing available technology protection measures that block or filter 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. Monitor 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:[2]

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

2. Cyberbullying awareness and response.[7][11]

Guidelines

Scope

This policy applies to all school district information technology resources and systems, including but not limited to, district-wide, school administered, department administered, or school district based entities. Use of any school district information technology resources and systems in any way or manner including utilization or access from equipment or source not managed or maintained by the school district is within the scope of and governed by this policy. Use of any school district IT resources or systems, even utilized with or accessed by a privately owned computer that is not managed or maintained by the district, is governed by this policy.

School District IT Resources and Systems

IT resources and systems include, but are not limited to, the computers, terminals, printers, networks, communication equipment, online and offline storage media and related equipment, software, and data files that are owned, managed, or maintained by the school district. IT resources and systems also include, but are not limited to, the district Intranet, the Internet, email, instant messaging and other network resources.

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.

Electronic Mail (email)

The district provided email is the official email of record for the district and should be used for all official business.

Students may be given access to district-provided student mail.

Guests/Contractors are not automatically eligible for a district email account. Email or network access accounts may be granted if directly sponsored by a district administrator.

All electronic systems, hardware, software, temporary or permanent files and any related systems or devices used in the transmission, receipt or storage of email are the property of the district. Email messages are considered to be district property and may be retrieved, if necessary, from individual computers even though deleted by the sender and receiver. Email communications that qualify as district records shall be maintained in accordance with applicable policy, administrative regulations and/or retention schedule(s).

Use of the district email system is subject to all applicable laws, regulations and policies.

Electronic Communications With Students and Social Media

Employees who communicate electronically with students via personal or District equipment/software; i.e. personal cell phone, home phone, home computer, District phone, District cell phone, District computer, etc., must do so in accordance with Policy 352 Electronic Communications with Students and Policy 901 Public Relations Objectives: District Use of Social Media, if applicable.[12]

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. Network users shall not reveal personal information to other users on the network, including chat rooms, email, social networking websites, etc.

Internet safety measures shall effectively address the following:[2][13]

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. Facilitating illegal activity.
2. Commercial or for-profit purposes.
3. Nonwork or nonschool related work.
4. Product advertisement or political lobbying.
5. Bullying/Cyberbullying.[7][11]
6. Hate mail, discriminatory remarks, and offensive or inflammatory communication.
7. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials.
8. Accessing, sending, receiving, transferring, viewing, sharing or downloading obscene, pornographic, lewd, or otherwise illegal materials, images or photographs.[14]
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 modification of materials in violation of copyright laws. [15]
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. Accessing the Internet, district computers or other network resources without authorization.
19. Disabling or bypassing the Internet blocking/filtering software without authorization.
20. 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 other than approved district staff.
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.[15][19]

District Website

The district may 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.

Users shall not copy or download information from the district website and disseminate such information on unauthorized web pages without authorization from the Superintendent or designee.

Consequences for Inappropriate Use

The network user shall be responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts.[9]

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. **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.

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.[3][4][20]

Legal

1. 20 U.S.C. 6777
2. 47 U.S.C. 254
3. Pol. 218
4. Pol. 233
5. Pol. 103
6. Pol. 104
7. Pol. 249
8. Pol. 218.2
9. 24 P.S. 4604
10. 24 P.S. 4610
11. 24 P.S. 1303.1-A
12. Pol. 901
13. 47 CFR 54.520
14. Pol. 237
15. Pol. 814
16. 18 U.S.C. 2256
17. 18 Pa. C.S.A. 6312
18. 18 Pa. C.S.A. 5903
19. 17 U.S.C. 101 et seq
20. Pol. 317
21. Pol. 103.1

24 P.S. 4601 et seq

Pol. 220

815-AR-1-RprtFormForComplnts-F-8-23-17.pdf (19 KB)

815-AR-2-RprtFormForInadvAccess-F-8-23-17.pdf (29 KB)

815-AR-3-ImplementationPlans-F-8-23-17.pdf (23 KB)

815-AR-4-CyberbullyingSocialNetwrkingEd-F-8-23-17.pdf (24 KB)

815-AR-5-EmailUse-F-8-23-17.pdf (27 KB)