Book	Policy Manual
Section	800 Operations
Title	Acceptable Use of Internet, Computers and Network Resources
Code	815
Status	Active
Adopted	January 8, 2024
Last Revised	October 21, 2024

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. To the extent the district provides E-Rate-funded Wi-Fi hotspots and services for off-premises use, the goal of the lending program is to provide broadband access to students and school staff who may need it. Off-premises use must be integral, immediate and proximate to the education of students and is subject to the requirements of the Children's Internet Protection Act.

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:[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

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 use of computers and network resources 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, delete, 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 Internet Service Provider (ISP), local, state and federal officials in any investigation concerning or related to the misuse of the district's Internet, computers and network resources.[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 materials, 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, or profane.
3. Threatening.[9][10]
4. Harassing or discriminatory.[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.[2][3][16]

Upon request by students or staff, the Superintendent or designee shall expedite 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, building administrators may authorize the temporary disabling of 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 Internet blocking/filtering software for a student's use. If a request for temporary disabling of 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 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.[16]

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 uses monitoring systems to monitor and detect inappropriate use and tracking systems to track and recover lost or stolen equipment.

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. Each student who receives an account will take part in a discussion with designated staff pertaining to proper use of the network.

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 and system administrators shall make initial determinations of whether inappropriate use has occurred, and their decision is final.

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:[2][3][16]

1. Utilizing a technology protection measure that blocks or filters 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:[3]

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

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

Because the district provides access to the Internet, students and their parents/guardians understand that the district and the system administrators have no control over content. The district will provide student access to Internet resources only in supervised environments and has taken steps to prevent access to objectionable or illegal material, but recognizes that potential dangers remain. Recognizing the existence of objectionable or illegal materials, the district and the system administrators do not condone accessing such materials and do not

permit usage of such materials in the school environment. Students who knowingly bring such materials into the school environment will be subject to appropriate disciplinary action, as outlined in this policy.

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:[3][16]

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. [19][20]

5. Restriction of minors' access to materials harmful to them.

Use of Personal Electronic Devices

The use of personal electronic devices on the district network is permitted only on designated networks. When a user connects a personal electronic device to a district network or district technology resources, this policy and its guidelines apply. Users are subject to the same levels of monitoring and access as if a district-owned device were being utilized. Users who connect a personal electronic device to a district network explicitly waive any expectation of privacy in the content exchanged over the district technology resources. Further, the district may decrypt any communications or internet traffic to ensure adherence to this policy.

Privacy

The district reserves the right to monitor any user's utilization of district technology resources. Users have no expectation of privacy while using district technology resources whether on or off district property. The district may monitor, inspect, copy, and review any and all usage of district technology resources including information transmitted and received via the Internet to ensure compliance with this and other district policies, and state and federal law. All e-mails and messages, as well as any files stored on district technology resources may be inspected at any time for any reason. Further, the district may decrypt any communications or internet traffic to ensure adherence to this policy.

District Provided Resources

District technology resources may be assigned or allocated to an individual user for his or her use. Despite being allocated to a particular user, the technology resources remain the property of the district and may be revoked, suspended, or inspected at any time to ensure compliance with this and other district policies. Users do not have an expectation of privacy in any district provided technology resource or any of its contents.

Prohibited Conduct

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. Bullying/Cyberbullying.[14][17]

2. Accessing, sending, receiving, transferring, viewing, sharing or downloading obscene, pornographic, lewd, or otherwise illegal materials, images or photographs.[21]

3. Access by students and minors to material that is harmful to minors or is determined inappropriate for minors in accordance with Board policy.

4. Transmission of material likely to be offensive or objectionable to recipients.

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.

8. Obtaining system privileges to which one is not authorized, including using another person's account name and password.

9. Permitting another person to use your account name and password.

10. Deliberately attempting to disrupt the performance of the district's computer system(s) or to destroy data by spreading computer viruses or by any other means.

11. Use of any district computer or information system to facilitate, advocate, condone or participate in illegal activities.

12. Use of any district computer or information system for personal or private commercial or financial gain.

13. Use of any district computer or information system to make unauthorized purchases of products and/or services inconsistent with current district purchasing policies and procedures.

14. Use of any district computer or information system for nonschool related work.

15. Use of any district computer or information system for nonschool related fundraising.

16. Use of any district computer or information system for political campaigning and/or lobbying.

17. Use of inappropriate language on any district computer or information system including, but not limited to, that which is obscene, profane, lewd, vulgar, rude, disrespectful, threatening or inflammatory as determined by the appropriate supervisor.

18. Use of any district computer or information system for hate mail, discriminatory remarks and false or defamatory material about a person or group.

19. Displaying or generating images, sounds or messages (on screen, computers or printers) which could create an atmosphere of discomfort, intimidation or harassment to others.

20. Violations of privacy including, but not limited to, revealing personal information about others.

21. Use of any district computer or information system to disrupt the work of others such as, but not limited to, intentionally obtaining or modifying files, passwords and/or data belonging to other users.

22. Unauthorized use of a network address, use of pseudonyms or anonymous use.

23. Copyright infringement or plagiarism. Students, staff and other users should assume that all works, including, but not limited to web designs, on the Internet are protected by the copyright laws and, thus, should make every attempt to request permission from the creator or shall cite or document the source.[22]

24. Loading or use of unauthorized software, games, programs, files or other electronic media.

25. Creating and sending or forwarding electronic chain letters.

26. Spamming, which is sending annoying, unnecessary and/or unsolicited electronic messages.

27. Actions which constitute the unauthorized copying, cross assembling or reverse compiling of programs and data provided by the district.

28. Destruction, modification, abuse or removal from the district of any piece of computer hardware, software or network system.

29. Wastefully using finite resources, such as paper, ink and electronic memory resources.

30. Posting for unauthorized or inappropriate use personal contact information about themselves or others including, but not limited to, home address, school address, work address, telephone numbers, email address, etc.

Online Conduct

Teachers and students using Web 2.0 resources are expected to treat blogspaces, wikispaces and podcast spaces as classroom space. Speech that is inappropriate for class is not appropriate for blogs. Users will conduct themselves in a manner reflective of a representative of the district. To ensure quality and appropriateness of content, all spaces will be monitored by the creator and/or moderator as well as the designated district employee on a regular basis. All blogs, wikis and podcasts will be secured with passwords to ensure safety and protect the identity of the participants.

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:[20][23]

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.[22][24]

Software Libraries

Software is provided to students as a curricular resource. No student may install, update, or download software without the expressed consent of the system administrator. Any software having the purpose of negatively impacting other members' accounts, software, hardware, or the district network (e.g., computer viruses) is specifically prohibited. They system administrators, at their sole discretion, reserve the right to refuse the posting of files and to remove files. The system administrators, at their sole discretion, further reserve the right to immediately terminate the account or take other appropriate disciplinary action.

Electronic Mail

Electronic mail (email) is a private electronic message sent by or to a user in correspondence with another person having Internet mail access. Messages received by the system are retained on the system until deleted by the recipient or until they reach the expiration date set by the system administrator.

A canceled district account will not retain its mail. Users are expected to remove old messages in a timely fashion. The system administrators may remove such messages if not attended to regularly by the user.

The district will provide email accounts to all staff and students who require them for curricular or professional purposes. These accounts are for educational use only. Business, personal entertainment, or other noneducational use is to be avoided. Student use of outside mail accounts or web-based email is prohibited.

Accessing outside or web-based accounts without teacher supervision and permission is a violation of this policy.

Personal Technology Equipment and Devices

The use of personally owned technology equipment in conjunction with the district's network or equipment could be a potential hazard to the district's network or equipment. These threats include breach of security and irreparable damages to the district's equipment, all of which may result in costs to the district including installation and maintenance costs.

In an effort to minimize risk, the district does not permit the connection of personally owned equipment to the district resources. This includes but is not limited to printers, scanners, digital cameras, external storage devices, notebooks, mice, keyboards, etc. Personally owned equipment can only be connected with the expressed permission of the building principal and Director of Technology after a review of the equipment and determination of compatibility by the Technology Department. Personally owned equipment will not be supported by the Technology Department and the district is not responsible for loss or damage to any personally owned equipment.

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.[25][26]

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.

Links

The links in the STSD website will allow users to leave the site. The linked sites are not under the control of the district and the district is not responsible for the contents of any linked site, any link contained in a linked site, or any changes or updates to such sites. The district provides these links only as a convenience, and the inclusions of any link does not imply endorsement of the site by the district.

Confidentiality

The district shall not reveal a student's personal identity or post a picture of a student on the network unless the student and his/her parent/guardian has given written consent. No confidential information concerning students or staff shall be transmitted over the system unless via a password protected system. All web pages created by students and staff will be subject to treatment as district-sponsored publications. Accordingly, the district reserves the right to exercise editorial control over such publications.[26]

COPPA

The district shall adhere to the requirements of the Children's Online Privacy Protection Act and shall obtain written parental permission to create accounts for children under the age of thirteen (13).[25]

Consequences for Inappropriate Use

The network user shall be responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts.[14]

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.[6][7][8]

Improperly restricting users from using network resources will be referred to the administration for appropriate disciplinary action.

Legal

1. 18 U.S.C. 2256
2. 18 Pa. C.S.A. 6312
3. 20 U.S.C. 7131
4. 47 U.S.C. 254
5. 18 Pa. C.S.A. 5903
6. Pol. 218
7. Pol. 233
8. Pol. 317
9. 24 P.S. 1302-E
10. Pol. 236.1
11. Pol. 103
12. Pol. 104
13. Pol. 103.1
14. Pol. 249
15. Pol. 218.2
16. 24 P.S. 4604
17. 24 P.S. 4610
18. 24 P.S. 1303.1-A
19. Pol. 113.4
20. Pol. 830
21. Pol. 237
22. Pol. 814
23. Pol. 800
24. 17 U.S.C. 101 et seq
25. Pol. 815
26. Pol. 815.1

24 P.S. 4601 et seq

18 Pa. C.S.A. 2709

Pol. 113.1

Pol. 220

Pol. 816

Pol. 824