Book	Policy Manual
Section	800 Operations
Title	Acceptable Use of Internet, Computers and Network Resources
Code	815
Status	Active
Adopted	June 24, 2019
Last Revised	April 15, 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.

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]

Computer - for purposes of this policy, district computers include any electronic device owned or leased by the district that has the capability to create, play or edit text, audio and video data; transmit or receive messages, text, data or images; operate software or online applications; or provide a wired or wireless connection to the Internet.

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.

Incidental Personal Use - use by an individual employee for occasional, personal communications. Personal use must comply with this policy and all other applicable policies, administrative regulations, procedures and rules, and may not interfere with the employee's job duties and performance, with the system operations, or with other system users. Under no circumstances should the employee believe his/her use is private. The district reserves the right to monitor, access and use of its network and electronic communications systems.

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 district Internet, 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, delete, access, receive or display on or over the district's Internet, computers or network resources, including personal files. The district reserves the right to monitor, track and log network access and use on district computers and network resources; monitor fileserver space and file storage 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 building principal or designee.

The Board establishes the following list of subject areas as inappropriate matter, in addition to those stated in law and defined in this policy, which shall not be accessed by minors:[4]

1. Hate speech.[9][10]

2. Lewd, vulgar or profane.

3. Threatening.[11][12]

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

5. Bullying.[14]

6. (Consisting of/Relating to) Weapons.[15]

7. Terroristic.[16]

8. Defamatory.

The district reserves the right to restrict access to any Internet sites or network functions it deems inappropriate through established Board policy, or the use of software and/or online server blocking/filtering. Specifically, the district operates and enforces a technology protection measure(s) that blocks or filters access to inappropriate matter by minors on its computers and network resources used and accessible to adults and students. The technology protection measure shall be enforced during use of computers and network resources with Internet access.[3][4][17]

Upon request by students or staff, the Superintendent or designee shall expedite a review and may authorize the adjustment of technology protection measures to enable access to material that is blocked or filtered but is not prohibited by this policy.[17]

Upon request by students or staff, building administrators may authorize the temporary adjustment of technology protection measures to enable access for bona fide research or for other lawful purposes. Written permission from the parent/guardian is required prior to adjusting Internet blocking/filtering for a student's use. If a request for temporary adjustment of technology protection measures is denied, the requesting student or staff member may appeal the denial to the Superintendent or designee for expedited review.[3][18]

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.[17]

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.

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 principals shall make initial determinations of whether inappropriate use has occurred, and may consult with the Superintendent or designee and the school solicitor when necessary.

The Superintendent or designee shall be responsible for recommending technology and developing procedures used to determine whether the district's computers and network resources 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][19]

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 on district computers and network resources.

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][20]

Guidelines

District computers and network accounts shall be used only by the authorized user of the computer or 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, building administrator or other appropriate school staff. Network users shall not reveal personal information to other users on the network or Internet, including chat rooms, email, social networking websites, etc.

Internet safety measures shall effectively address the following:[4][19]

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, social networking websites 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.[21][22][23]
5. Restriction of minors' access to materials harmful to them or which have been designated as inappropriate matter in Board policy.

Prohibitions

Users are expected to act in a responsible, ethical and legal manner in accordance with Board policy, accepted rules of network etiquette and federal and state law and regulations. Specifically, the following are prohibited uses of district computers and/or network resources:

1. Facilitating illegal activity.
2. Commercial or for-profit purposes.
3. Nonwork or nonschool related work.
4. Product advertisement.
5. Bullying/Cyberbullying.[14][20]
6. Hate mail, discriminatory remarks, harassment and offensive or inflammatory communication.[9][10][14][24]
7. Unauthorized or illegal installation, distribution, reproduction or use of copyrighted materials.[25]
8. Accessing, sending, receiving, transferring, viewing, sharing or downloading obscene, pornographic, lewd or otherwise illegal materials, images or photographs.[26]
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. Vulgar language or profanity.
11. Transmission of material that a reasonable person would know 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.[25]

15. Loading or accessing 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, systems and files.
18. Accessing the Internet, district computers or other network resources without authorization.
19. Disabling, adjusting or bypassing the Internet blocking/filtering technology protection measure(s) without authorization.
20. Accessing, sending, receiving, transferring, viewing, sharing, deleting or downloading confidential information without authorization.

Security

System security is protected through the use of passwords and/or encryption and district security procedures. 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:[23][27][28]

1. Employees, students and other authorized users shall not reveal their passwords to another individual.
2. Users are not to use a computer that has been logged in under another user.
3. Any user identified as a security risk or having a history of problems with other computers or network systems may be denied access to the district's computers and network resources.

Copyright

The illegal use of copyrighted materials is prohibited. Any data uploaded to or downloaded from the network or Internet shall be subject to fair use guidelines and applicable laws and regulations.[25][29]

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 authorized users publishing content on the district website shall receive appropriate training and 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 building principal.

Accessibility –

District staff who maintain district websites and web pages shall post content which is accessible to individuals with disabilities, to the same extent that it is available to other users, based on the needs of the individuals and limitations of the platform. This shall include, but is not limited to:[9][10][13][30][31][32]

1. Including alternate text descriptions or captions for images.
2. Including captions for video content.
3. Avoiding text that is posted as an image or conveyed using only color cues.
4. Creating links and attachments in formats that are accessible to screen readers and other assistive technology, and may be accessed through keyboard or speech navigation.
5. Formatting text so that it is accessible to screen readers and other assistive technology, and may be accessed through keyboard or speech navigation.

All district websites shall contain clear contact information that may be used by members of the public to request accommodations or assistance.

Consequences for Inappropriate Use

Users of district computers and network resources shall be responsible for damages to the equipment, systems, platforms and software resulting from deliberate or willful acts.[17]

Illegal use of the district computers and network resources; 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 and Board policies for behavior and communications apply when using the district computers, network resources and Internet, in addition to the stipulations of this policy.

Vandalism shall result in loss of access privileges, disciplinary action and/or referral to legal authorities. **Vandalism** is defined as any malicious attempt to harm or destroy data of another user, the district, the 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 referral to legal authorities.[6][7][8]

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. Pol. 103

10. Pol. 104

11. 24 P.S. 1302-E

12. Pol. 236.1

13. Pol. 103.1

14. Pol. 249

15. Pol. 218.1

16. Pol. 218.2

17. 24 P.S. 4604

18. 24 P.S. 4610

19. 47 CFR 54.520

20. 24 P.S. 1303.1-A

21. Pol. 113.4

22. Pol. 216

23. Pol. 830

24. Pol. 247

25. Pol. 814

26. Pol. 237

27. Pol. 800

28. Pol. 830.1

29. 17 U.S.C. 101 et seq

30. 42 U.S.C. 12101 et seq

31. 29 U.S.C. 794

32. 28 CFR 35.160

24 P.S. 4601 et seq

18 Pa. C.S.A. 2709

Pol. 113.1

Pol. 220

Pol. 816

Pol. 824

STUDENT ACCEPTABLE USE OF
COMPUTER NETWORK/INTERNET AGREEMENT

Please read carefully the Muncy School District Acceptable Use of Internet, Computers and Network Resources (Policy No. 815).

I understand and will abide by the Network and Internet Use Rules. I further understand that violation of the regulations will not be acceptable and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked and appropriate school disciplinary action and/or legal action may be taken.

Student Name (please print)

Student's Signature

Date

As parent/guardian of this student, I understand that network access is designed for the purpose of improving instruction and learning and that the Muncy School District cannot restrict access to all controversial material. I will not hold the School District responsible for materials this student may acquire on the network. Further, I accept full responsibility for supervision if and when my child's use is not in a school setting. I hereby give my permission for an account to be issued in the name of the student named above and certify that the information in this agreement is correct.

Parent/Guardian (please print)

Parent/Guardian Signature

Date