Mars Area School District
545 Route 228; Mars, Pa. 16046
Ph: (724) 625-1518 or (724) 625-9030
Fax: (724) 625-1060
Website: www.marsk12.org

Book	Policy Manual
Section	800 Operations
Title	Acceptable Use of Internet, Computers and Network Resources
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 24 P.S. 4601 et seq Pol. 220
Adopted	July 19, 2016

Purpose

The Board supports use of the computers, Internet and other network resources in the District's instructional and operational programs 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

Computer Network includes all local area networking and wide-area networking within the school community as well as all on-line and direct-wired networking such as the Internet to which the school network may be linked.

Telephone Network includes all telephones and lines and hardware connecting telephones within the school community as well as all direct-wired connections to service providers.

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

The term, **Child Pornography**, is defined under both federal and state law.

Under Federal law, **Child Pornography** 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.

Under State law, **Child Pornography** 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.

Under Federal law, **Harmful to Minors** 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.

Under state law, **Harmful to Minors** 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 is 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.

Vandalism is 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.

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. 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:

1. Monitor, track, and log network access and use;

2. Monitor file server space utilization by District users; or

3. Deny access to prevent unauthorized, inappropriate or illegal activity and 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.
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 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]

All 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 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:[3][4][18]

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:[4]

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

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

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. Network users shall not reveal personal information such as addresses and phone numbers to other users on the network, including chat rooms, e-mail, social networking websites, etc.

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 e-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. Non-work or non-school related work.
4. Product advertisement or political lobbying.
5. Bullying/Cyberbullying.[14][19]
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.[20]
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.[21]
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.
21. Quoting personal communications in a public forum without the original author's prior consent.
22. Unauthorized disclosure or dissemination of another person's personal information, including address of residence, telephone number, e-mail address, photograph, password, etc.
23. Deliberate wasting of network resources, such as unnecessary or frivolous traffic, placing a program in an endless loop, excessive printing, etc.
24. Dissemination of chain letters or similar materials encouraging such messages to be further disseminated to multiple recipients.

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.

Copyrights

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.

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.

District Telephone Networks

The use of the District's telephone network must be in support of education or for safety and security matters. Use of the network must comply with rules appropriate for that network. Network accounts, including voicemail, are to be used by the authorized owner of the account for authorized purposes.

The determination as to whether a use is appropriate lies solely within the discretion of the District. The use of the telephone network for illegal, inappropriate or unethical purposes by students or employees is prohibited. More specifically, the following uses are prohibited:

1. Use of the telephones to facilitate illegal activity.
2. Use of the telephones for commercial or for-profit purposes.
3. Use of the telephones for non-work or non-school related work during any period of time when staff members are assigned to an instructional or supervisory assignment. Except in the event that an employee has a reason to expect an emergency call, ringers on telephones are to be switched off during all periods when the teacher is scheduled to provide instruction or supervision to students.
4. Use of telephones for product advertisement or political lobbying.
5. Use of telephones for hate or discriminatory remarks and offensive or inflammatory communication.
6. Use of telephones to access obscene or pornographic communications.
7. Use of inappropriate language or profanity on the network.
8. Use of the network to transmit communications likely to be offensive or objectionable to recipients.
9. Impersonation of another user.
10. Use of the network to disrupt the work of other users.
11. Destruction, modification or abuse of telephones or other network hardware.

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]

815 Attachment 1 - Computer Networks-Internet Use Student Agreement.pdf (145 KB)

815 Attachment 2 - Computer Networks-Internet Use Employee Agreement.pdf (142 KB)