Mountain View School District

Book	Policy Manual
Section	800 Operations
Title	Acceptable Use of Technology and the Internet
Number	815
Status	Active
Adopted	February 8, 2010
Last Revised	August 14, 2017

Purpose

The district provides employees, students, and guests with access to the district's network and to the Internet, whether wired or wireless, in order to facilitate learning, teaching and daily operations through interpersonal communications and access to information, research and collaboration.

Access to the district's network shall be for specific district-related purposes to access information and research; to collaborate; to facilitate learning and teaching; and to foster the educational mission, vision, and beliefs of the school district.

Authority

The electronic information available to students and staff 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 school district operates and enforces technology protection measures that filter online activities of all users so as to filter or block inappropriate matter on the Internet.[1][2]

The district shall not be responsible for any unauthorized charges or fees resulting from access to the Internet.

Users have no privacy expectations in the contents of their personal files or any of their use of the school district's network. The school district reserves the right to monitor, track and/or log user access, as well as monitor and allocate fileserver space and access all user files.

The district establishes that network use is a privilege, not a right; inappropriate, unauthorized, and illegal use will result in cancellation of those privileges and appropriate disciplinary action. The school district will cooperate to the extent legally required with Internet Service Provider (ISP), local, state, and federal officials in any investigation concerning or related to the misuse of the district's network.

Definitions

Child Pornography - under federal law, 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:[8]

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.

3. Such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

Under Pennsylvania law, 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.[9]

Computer - includes any district-owned, leased, or licensed or user-owned personal hardware, software, or other technology used on district premises or at district events, or connected to the district network, containing district programs or school district or student data including images, files, and other information attached or connected to, installed in, or otherwise used in connection with a computer. **Computer** includes, but is not limited to desktop; notebook; Chromebooks; power book; tablet PC or laptop computers; printers; cables; other peripherals, including thumb and flash drives; specialized electronic equipment used for students' special educational purposes; global positioning system (GPS) equipment; cell phones, with or without Internet access and/or recording and/or camera/video and other capabilities; mobile phones, or wireless devices; two-way radios/telephones; paging devices; laser pointers and attachments; and any other such technology developed.[3]

Harmful to Minors - under federal law, any picture, image, graphic image file or other visual depictions that:[1][2]

1. Taken as a whole, with respect to minors, appeals to the 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 content, actual or simulated normal or perverted sexual acts, or lewd exhibition of the genitals.

3. Taken as a whole lacks serious literary, artistic, political, educational or scientific value as to minors.

Under Pennsylvania law, any depiction or representation in whatever form, of nudity, sexual conduct, sexual excitement, or sadomasochistic abuse, when it:[10]

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.

3. Taken as a whole, lacks serious literary, artistic, political, educational or scientific value for minors.

Minor - for purposes of compliance with the Children's Internet Protection Act (CIPA), an individual who has not yet attained the age of seventeen (17). For other purposes, **minor** shall mean the age of minority as defined in the relevant law.[2]

Network - a system that links two (2) or more computer systems, including all components necessary to effect the operation, including, but not limited to: computers, copper and fiber cabling, wireless communications and links, equipment closets and enclosures, network electronics, telephone lines, printers and other peripherals including thumb and flash drives, storage media, software, and other computers and/or networks to which the network may be connected, such as the Internet or those of other institutions.

Obscene - under federal law, analysis of the material meets the following elements:

1. Whether the average person, applying contemporary community standards, would find that the material, taken as a whole, appeals to the prurient interest.

2. Whether the work depicts or describes, in a patently offensive way, sexual conduct specifically designed by the applicable state or federal law to be obscene.

3. Whether the work taken as a whole lacks serious literary artistic, political, educations, or scientific value.

Under Pennsylvania law, analysis of the material meets the following elements:[10]

1. The average person, applying contemporary community standards, would find that the material, 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.

3. The subject matter, taken as a whole lacks serious literary, artistic, political, educational or scientific value.

Proxy Server - a server that can be used to control and speed up access to the Internet. It can also allow multiple computers in a network to access the Internet by using a single IP address.

Sexual Act and Sexual Contact - as defined at 18 U.S.C. Sec. 2246, and at 18 Pa. C.S.A. Sec. 5903. [10][11]

Technology Protection Measure(s) - a specific technology that blocks or filters Internet access to visual depictions that are obscene, child pornography or harmful to minors.[2]

Visual Depictions - undeveloped film and videotape and data stored on computer disk or by electronic means which is capable of conversion into a visual image but does not include mere words. [8]

Delegation of Responsibility

The district shall make every effort to ensure that network resources are used responsibly by students and staff. These resources may include, but are not limited to network user accounts, computers, the Internet, email, blogs, and other second-generation web services. The Superintendent or designee will serve as the coordinator to oversee the school district's network and will work with others to educate users, approve activities, maintain executed user agreements, and interpret and enforce this policy.

The Superintendent will direct the district computer technicians to establish and maintain a process of setting up user accounts, establish quotas for fileserver storage space, establish a document and email retention procedure, as well as a virus protection process.

The district reserves the right to restrict access to any Internet sites or functions it may deem inappropriate through general policy, software blocking or online server blocking. Specifically, the district operates and enforces technology protection measure(s) that block or filter online activities of minors or its computers used and accessible to adults and students so as to filter or block inappropriate matter on the Internet. **Inappropriate matter** includes, but is not limited to visual, graphic, text and any other form of obscene, sexually explicit, child pornographic, or other material that is harmful to minors, or that are hateful; illegal; defamatory; lewd; vulgar; profane; rude; inflammatory; threatening; harassing; discriminatory as it pertains to race, color, religion, national origin, gender, marital status, age, sexual orientation, political beliefs, receipt of financial aid, or disability; violent; bullying; terroristic; and advocate the destruction of property. Measures designed to restrict adults' or minors' access to material harmful to minors may be disabled to enable an adult or student to access bona fide research, not within the prohibitions of this policy, or for another lawful purpose. No person may have access to material that is illegal under federal or state law.[1][2][12]

Expedited review and resolution of a claim that the policy is denying a student or adult to access material will be enforced by an administrator, supervisor, or their designee upon the receipt of a written consent from a parent/guardian for a student, and upon the written request from an employee.

Administrators, teachers, and staff have the responsibility to work together to help students develop the skills and judgment required to make effective and appropriate use of network resources. This includes educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response. All users have the responsibility to respect the rights of all other users within the school district and to abide by the rules established by the school district, local, state and federal laws. The school district will notify parents/guardians annually about the network systems and the policies governing their use. A copy of this policy shall be posted on the district's website, published for reference in the annual student handbook, and available directly from the Office of the Superintendent.[4][12]

Guidelines

Parental Notification and Responsibility

The district will notify the parents/guardians about the district's computer information system and the policies governing their use. This policy contains restrictions on accessing inappropriate material. There is a wide range of material available on the Internet, some of which may not be fitting with the particular values of the families of the students. It is not practically possible for the school district to monitor and enforce a wide range of social values in student use of the Internet. Further, the school district recognizes that the parents/guardians bear primary responsibility for transmitting their particular set of family values to their children The district will encourage parents/guardians to specify to their children what material is and is not acceptable for their children to access through the district's computer information system.

School District Limitation of Liability

The district makes no warranties of any kind, either expressed or implied, that the functions or the services provided by or through the district's computer information system will be error-free or without defect. The district does not warrant the effectiveness of Internet filtering. The electronic information available to users does not imply endorsement of the content by the school district. The district is neither responsible for nor guarantees the accuracy or quality of the information obtained through or stored on the computer information system. The district shall not be responsible for any damage users may suffer, including but not limited to, information that may be lost, damaged, delayed, misdelivered, or unavailable when using the computers, network, and electronic communications systems. The district shall not be responsible for material that is retrieved through the Internet, or the consequences that may result from them. The district shall not be responsible for any unauthorized financial obligations, charges, or fees resulting from access to the district's computer information system. In no event shall the school district be liable to the user for any damages whether direct, indirect, special, or consequential, arising out of the use of the computer information system.

The Superintendent or designee shall determine what is inappropriate use based on district guidelines. The building administrator shall notify the Superintendent when issues outside the guidelines are encountered.

The Superintendent or designee shall be responsible for implementing technology and procedures to determine whether the district's computers are being used for purposes prohibited by law or in violation of this policy. Because of the nature of the technology that allows the Internet to operate, the school district may not be able to completely block access to these explicit materials. Accessing these and similar types of resources may be considered an unacceptable use of school resources and may result in disciplinary actions and/or denial of Internet privileges.[1][2][6][13][14][15][16]

The procedure shall include but not be limited to:[1][2]

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.

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

Prohibitions

Students and staff 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. Illegal activity.

2. Communication focused on nonwork or nonschool related topics. This includes commercial or for-profit purposes.

3. Communication of private/personal information of others.

4. The purchase or sale of any product or service.

5. Participation in online auctions or online gaming and/or gambling.

6. Product advertisement or political lobbying.

7. Hate mail, discriminatory remarks and offensive, inflammatory, or inappropriate communication (relay chat, news groups, email, blogs, social networking sites, etc.).

8. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials.

9. Access (send, receive, view, download, or transmit) to sexually suggestive, sexually explicit, obscene or pornographic material or child pornography.[3]

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

11. Use of inappropriate language or profanity.

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

13. Intentional use, retrieval or modification of files, passwords, and data belonging to other users.

14. Impersonation of another user, anonymity, and pseudonyms.

15. Fraudulent reproduction, communication, or modification of materials in violation of copyright laws.[7]

16. Use of unauthorized games, programs, files, or other electronic media.

17. Disruption of the work of other users.

18. Destruction, modification, abuse, or unauthorized access to network hardware, software, and files.

19. Quotation, summarization, or other recounting of personal communications in a public forum without the original author's prior consent.

20. Cyberbullying or any other type of harassment prohibited by law, the Student Code of Conduct, or Board policy.[4][5]

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, the following guidelines shall be followed:

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

2. Users may not use a computer that has been logged in under another student's or employee's name. If a previous user has not logged off, the current user must immediately log out and then log back in under his/her own name and password.

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.

4. Users must create passwords that follow the guidelines for required syntax.

Consequences for Inappropriate Use

The network user shall be responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts.[12]

Illegal use of the network, intentional deletion or damage to files of data belonging to others, copyright violations, and theft of services will be reported to the appropriate legal authorities.

General rules for behavior and communications apply when using the Internet, in addition to the stipulations of this policy. Loss of access and/or disciplinary actions shall be consequences for inappropriate use.

Vandalism will result in cancellation of access privileges. **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.

Copyright

Federal laws, cases, and guidelines will govern the use of material accessed through the district network.[7]

School district guidelines on plagiarism, as well as the Student Code of Conduct, will govern use of material accessed through the district network. The district's guidelines on plagiarism can be found in the Student Handbook at the beginning of each year. Teachers will instruct students in appropriate research and citation practices.

Safety

To the greatest extent possible, users of the network will be protected from harassment and unwanted or unsolicited communication. Any network user who receives threatening or unwelcome communications 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, Internet, etc.

Any district computer/server utilized by students and staff shall be equipped with Internet blocking/filtering software.[1][2]

Internet safety measures shall effectively address the following:[2][17]

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. Prevention of unauthorized disclosure, use, and dissemination of personal information regarding minors.
5. Restriction of minors' access to materials harmful to them.

Legal

1. 20 U.S.C. 6777
2. 47 U.S.C. 254
3. Pol. 237
4. Pol. 249
5. 24 P.S. 1303.1-A
6. Pol. 218
7. Pol. 814
8. 18 U.S.C. 2256
9. 18 Pa. C.S.A. 6312
10. 18 Pa. C.S.A. 5903
11. 18 U.S.C. 2246
12. 24 P.S. 4604
13. Pol. 233
14. Pol. 317
15. Pol. 417
16. Pol. 517
17. 47 CFR 54.520

24 P.S. 4601 et seq

17 U.S.C. 101 et seq

Pol. 103

Pol. 104

Pol. 218.2

Pol. 220

Pol. 248

Pol. 348

Pol. 448

Pol. 548

815-Attach.doc (28 KB)

Last Modified by Barb Maxon on August 21, 2017