Ferndale Area School District

Book	Policy Manual
Section	800 Operations
Title	Acceptable Use Of Internet, Computers and Network Resources
Code	815
Status	Active
Adopted	June 19, 1996
Last Revised	October 17, 2018

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 the purpose of accessing relevant information, research, to facilitate learning and teaching, and to foster the educational purpose and mission of the school district.

For instructional purposes, the use of network resources, internet and computers 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.

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, 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.[1][2][3]

It is often necessary to access user accounts in order to perform routine maintenance and security tasks. System administrators have the right to access user accounts, information, and communications for any reason in order to uphold this policy and to maintain the security of the system and integrity of the information stored therein. Users shall have no expectation of privacy in anything they create, store, send, delete, receive or display on or over the district's Computer Information System systems, including personal files or any use of the district's systems. The district reserves the right to monitor, track, and log network access and use; monitor and allocate fileserver space utilization by district users.

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 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.[4][5][6]

Upon request by 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.[4]

Upon request by 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 when needed for student presentation. Written permission from the classroom teacher and parent/guardian is required prior to disabling Internet blocking/filtering software for a student's use.[5][7]

Delegation of Responsibility

The Director of Education shall serve as technology coordinator to oversee the district's Computer Information Systems.

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.[4]

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.

Student user agreements shall also be signed by a parent/guardian. (Attachments)

Administrators, teachers and staff have a professional responsibility to work together to help students develop the intellectual skills and judgment necessary to be effective and appropriate consumers of online resources.

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/District Technology Coordinator shall have the authority to determine what is inappropriate use.

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:[5][6][11]

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 through the district current information technology service provider and reviewed with the Director of Education.

3. Monitoring online activities of minors.

The Superintendent or designee shall oversee administrative regulations that ensure students are educated on network etiquette and other appropriate online behavior, including:[6]

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

2. Cyberbullying awareness and response.[9][10]

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 to other users on the network, including chat rooms, email, social networking websites, etc.

Internet safety measures shall effectively address the following:[6]

1. Control of access by minors to inappropriate material on the Internet and World Wide Web.[11]

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. Sending unsolicited mass-email messages (Spam).
6. Bullying/Cyberbullying, communicating terroristic threats, discriminatory remark, hate mail, or harassing statements.
7. Creating obscene, vulgar, profane, lewd, pornographic, harassing, or terroristic materials, firearms, or drug paraphernalia. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials.
8. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials.
9. Accessing, sending, receiving, transferring, viewing, sharing or downloading obscene, pornographic, lewd, or otherwise illegal materials, images or photographs, or material that advocates illegal drug use.
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. Engaging in intentional acts which might threaten the health, safety, or welfare of any person(s).
12. Transmission of material likely to be offensive or objectionable to recipients.
13. Intentionally obtaining or modifying of files, passwords, and data belonging to other users.
14. Impersonation of another user, anonymity, and pseudonyms.
15. Fraudulent copying, communications, or modification of materials in violation of copyright laws.
16. Loading or using of unauthorized games, programs, files, or other electronic media.
17. The use of technology resources to gamble.
18. Disruption of the work of other users.
19. Destruction, modification, disruption, abuse or unauthorized access to network hardware, software, equipment, and files.
20. Accessing the Internet, district computers or other network resources without authorization.
21. Disabling or bypassing the Internet blocking/filtering software without authorization.
22. 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.

2. Students 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 Infringement and Plagiarism

Federal laws, cases, and guidelines pertaining to copyright will govern the use of material accessed through district resources. Users will make a standard practice of requesting permission from the holder of the work and complying with license agreements. Employees will instruct students to respect copyrights, request permission when appropriate, and comply with license agreements, and employees will respect and comply as well.

Violations of copyright law can be a felony, and the law allows a court to hold individuals personally responsible for infringing the law. The district does not permit illegal acts pertaining to the copyright law; therefore any user violating the copyright law does so at his/her own risk and assumes all liability.

Violations of copyright law include, but are not limited to, the making of unauthorized copies of any copyrighted material (such as commercial software, text, graphic images, audio and video recording), distributing copyrighted materials over computer networks, and deep-linking and framing into the content of others' websites. Further, the illegal installation of copyrighted software or files for use on the district's computers is expressly prohibited. This includes all forms of licensed software and electronic software downloaded from the Internet.

District guidelines on plagiarism shall govern use of material accessed through the district's systems. Users will not plagiarize works that they find. Teachers will instruct students in appropriate research and citation practices.

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.

Consequences For Inappropriate Use

The network user shall be responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts.[4]

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. The user may lose the privilege of district-provided technology and connectivity permission. Appropriate discipline will be assigned.

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.

Definitions

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.[1][2][3]

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:[14]

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.[15]

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:[5][6]

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:[16]

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:[16]

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.[6]

Legal

1. Pol. 218
2. Pol. 233
3. Pol. 317
4. 24 P.S. 4604
5. 20 U.S.C. 6777
6. 47 U.S.C. 254
7. 24 P.S. 4610
9. 24 P.S. 1303.1-A
10. Pol. 249
11. 47 CFR 54.520
12. Pol. 237
13. Pol. 814
14. 18 U.S.C. 2256
15. 18 Pa. C.S.A. 6312
16. 18 Pa. C.S.A. 5903

815-ATTACHMENT.pdf (178 KB)

815-AUP-PreK3-2-SIGNOFF.pdf (138 KB)

815-AUP-3-6-SIGNOFF-10-18.pdf (88 KB)

815-AUP-7-12-SIGNOFF-10-18.pdf (88 KB)

815-AUP-STAFF-SIGNOFF-08-22.pdf (18 KB)