FOX CHAPEL AREA SCHOOL DISTRICT

Book	Policy Manual
Section	800 Operations
Title	Acceptable Use of Electronic Information
Number	815
Status	Active
Adopted	May 10, 2010
Last Revised	June 11, 2012

Purpose

The Board supports use of the Internet and other computer networks 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.

For instructional purposes, the use of network facilities shall be consistent with the curriculum adopted by the school district as well as the varied instructional needs, learning styles, abilities, and developmental levels of students.

Authority

The use of the district's systems must be in compliance with the established policies, procedures, and conditions of the Fox Chapel Area School District and any external entity to which the network or electronic resources are connected.[11]

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

The district reserves the right to log network use and to monitor fileserver space utilization by district users, while respecting the privacy rights of both district users and outside users.

The Board establishes that network use and the use of all district electronic devices, including cell phones, is a privilege, not a right; inappropriate, unauthorized and illegal use will result in cancellation of those privileges and appropriate disciplinary action.

The Board shall establish a list of materials, in addition to those stated in law, that are inappropriate for access by minors.[1]

Delegation of Responsibility

The district shall make every effort to ensure that this resource is used responsibly by students and staff.

Administrators, teachers and staff have a professional responsibility to work together to help students develop the intellectual skills necessary to discriminate 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 and staff have the responsibility to respect and protect the rights of every other user in the district and on the Internet.

The building administrator shall have the authority to determine what is inappropriate use; his/her decision is final.

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 for accessing sexually explicit materials. The procedure shall include but not be limited to:[1][2][8]

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.

Guidelines

Network accounts shall be used only by the authorized owner of the account for its approved purpose. All communications and information accessible via the network should be assumed to be private property and shall not be disclosed. 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. Facilitating illegal activity.

2. Commercial or for-profit purposes.

3. Nonwork or nonschool related work during working hours.
4. Product advertisement or political lobbying.
5. Hate mail, discriminatory remarks, and offensive or inflammatory communication.
6. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials.
7. Access to obscene or pornographic material or child pornography.
8. Access by students and minors to material that is harmful to minors or is determined inappropriate for minors in accordance with Board policy.
9. Inappropriate language or profanity.
10. Transmission of material likely to be offensive or objectionable to recipients.
11. Intentional obtaining or modifying of files, passwords, and data belonging to other users.
12. Impersonation of another user, anonymity, and pseudonyms.
13. Fraudulent copying, communications, or modification of materials in violation of copyright laws.[3]
14. Loading or using of unauthorized games, programs, files, or other electronic media.
15. Disruption of the work of other users.
16. Destruction, modification, abuse or unauthorized access to network hardware, software and files.
17. Quoting of personal communications in a public forum without the original author's prior consent.

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. Passwords shall be at least eight (8) characters in length and contain at least one (1) numeric and special character. Passwords shall also be changed every thirty (30) days.
3. Users are not to use a computer that has been logged in under another student's or employee's name.

4. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the network.

Consequences for Inappropriate Use

The network user shall be responsible for damages to the equipment, systems, and software. Deliberate and/or negligent abuse of the network, computing resource, or any other district resource could lead to disciplinary action. Any such action will be subject to applicable district policies.[4][5][6][7]

Offenders may also be subject to criminal prosecution. Under Pennsylvania law, it is a felony punishable by fine of up to $15,000 and imprisonment of up to seven (7) years for any person to access, alter, or damage any computer system, networking, software, or database, or any part thereof, with the intent to interrupt the normal functioning of the organization. Knowingly and without authorization, disclosing a password to a computer system, network, etc. is a misdemeanor punishable by a fine of up to $10,000 and imprisonment of up to five (5) years, as is intentional and unauthorized access to a computer, interference with the operation of a computer or network, or alteration of computer software.

1. 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 for possible prosecution.

2. In the event there is an allegation that an individual has violated the district Acceptable Use Policy, the individual will be provided with a written notice of the alleged violation and be given an opportunity to present an explanation.

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

4. 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.

Search and Seizure

The district has the right to maintain and monitor all use of network activity. An individual search may be conducted if there is reasonable suspicion that a user has violated the district policy or the law. The investigation will be reasonable and related to the suspected violation.

All users should be aware that their personal files are discoverable under state public record laws.

Copyright

The illegal use of copyrighted software by students and staff is prohibited. Any data uploaded to or downloaded from the network shall be subject to fair use and TEACH Act guidelines of the copyright law and contain appropriate citation and attribution.[3][12][11]

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 such as personal addresses or telephone numbers to other users on the network, including chat rooms, e-mail, Internet, etc. Students will not agree to meet with someone they have met online without their parent's/guardian's approval. Students will promptly disclose to their teacher, administrator, or parent/guardian any messages received that are inappropriate or make students feel uncomfortable.

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

Internet safety measures shall effectively address the following:[1]

1. Control of access by minors to inappropriate matter on the Internet and World Wide Web.[8]

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.[1][9][10]

4. Unauthorized disclosure, use, and dissemination of personal information regarding minors.

5. Restriction of minor's access to materials harmful to them.

6. Educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.[1][9][10]

Legal

1. 47 U.S.C. 254
2. 20 U.S.C. 6777
3. Pol. 814
4. 24 P.S. 4604
5. Pol. 218
6. Pol. 233
7. Pol. 317
8. 47 CFR 54.520
9. 24 P.S. 1303.1-A
10. Pol. 249
11. Administrative Regulation - 815 AR, 814 AR
12. 17 U.S.C. 101 et seq

18 Pa. C.S.A. 5903

18 Pa. C.S.A. 6312

18 U.S.C. 2256

24 P.S. 4601 et seq

Pol. 103

Pol. 103.1

Pol. 104

Pol. 218.2

Pol. 220

Pol. 237

Last Modified by Donna Beley on January 29, 2018