Book	Policy Manual
Section	800 Operations
Title	Acceptable Use of Internet, Computers and Network Resources
Number	815
Status	Active
Adopted	May 18, 1995
Last Revised	August 3, 2017

Purpose

The Board of School Directors 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.

The School District of Haverford Township ("district") provides students, staff and other authorized individuals with conditional access to the district's computers, electronic communication systems and network, which includes Internet access.

The use of technology and network facilities shall be consistent with the curriculum adopted by the school district including the varied instructional needs, learning styles, abilities, and developmental levels of the students; as well as administrative and operational functions. Incidental personal use of school district electronic devices and network is permitted for users so long as such use does not interfere with work duties, educational practices, functions, system operations, or with other system users.

Users may also be permitted to use personal electronic devices while on school district property, at school district events and/or in connection with the school district's network systems, but only in strict compliance with this policy and all other applicable school district policies, procedures and rules, as well as Internet Service Provider ("ISP") rules and regulations and all applicable local, state and federal laws. Use of personal electronic devices must not interfere with educational practices, functions, system operations, or other system users, and/or otherwise damage or impair the school district's computer information systems.

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. Users are any student, staff member, or guest making authorized use of district computers, servers or network.

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 incurred by a user while accessing the Internet on any district technology nor for any losses or charges resulting from user's personal use of district technology.

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 monitor 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 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][4][5]

The district reserves the right to restrict access to any Internet sites or functions it deems inappropriate, or the use of software and/or online server blocking including technology protection measure(s) that blocks or filters access to inappropriate matter by Users.[6][7][8]

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.[7]

Users of district networks or district-owned equipment shall, prior to being given access or being issued equipment, sign user agreements, as required by the district, acknowledging awareness of the provisions of this policy, and awareness that the district uses monitoring systems to monitor and detect 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:[6][8][9]

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:[8]

1. Interaction with other individuals on social networking websites and in chat rooms.
2. Cyberbullying awareness and response.[10][11]

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:[8][9]

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

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-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where:[12]

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.[13]

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:[6][8]

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:[14]

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:[14]

1. The average person applying contemporary community standards would find that the subject matter taken as a whole appeal 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 is intended to blocks or filters Internet access to visual depictions that are obscene, child pornography or harmful to minors.[8]

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. Product advertisement or political lobbying.
4. Bullying/Cyberbullying.[10][11]
5. Hate mail, discriminatory remarks, and offensive or inflammatory communication.
6. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials.
7. Accessing, sending, receiving, transferring, viewing, sharing or downloading obscene, pornographic, lewd, or otherwise illegal materials, images or photographs.[15]
8. Intentional obtaining or modifying of files, passwords, and data belonging to other users.
9. Impersonation of another user, anonymity, and pseudonyms.
10. Fraudulent copying, communications, or modification of materials in violation of copyright laws.[16]
11. Loading or using of unauthorized games, programs, files, or other electronic media.
12. Disruption of the work of other users.
13. Destruction, modification, abuse or unauthorized access to network hardware, software and files.
14. Accessing the Internet, district computers or other network resources without authorization.
15. Disabling or bypassing the Internet blocking/filtering software without authorization.
16. 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. 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.

Copyright

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.[16][17]

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 district employees publishing content 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.[7]

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. **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.

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][4][5]

Legal

1. Pol. 218
2. Pol. 233
3. Pol. 317
4. Pol. 417
5. Pol. 517
6. 20 U.S.C. 6777
7. 24 P.S. 4604
8. 47 U.S.C. 254
9. 47 CFR 54.520
10. 24 P.S. 1303.1-A
11. Pol. 249
12. 18 U.S.C. 2256
13. 18 Pa. C.S.A. 6312
14. 18 Pa. C.S.A. 5903
15. Pol. 237
16. Pol. 814
17. 17 U.S.C. 101 et seq

24 P.S. 4601 et seq

Pol. 103

Pol. 104

Pol. 220

Pol. 248

Pol. 348

Pol. 448

Pol. 548

Staff Internet Agreement.docx (139 KB)

StudentAcceptableUsePolicy-SignaturePage.pdf (84 KB)