Book
Policy Manual

Section
800 Operations

Title
Acceptable Use of Computer Networks and Equipment

Number
815

Status
Active

Legal
2. 20 U.S.C. 6777
3. 47 U.S.C. 254
4. Pol. 218
5. Pol. 233
6. Pol. 317
7. 20 U.S.C. 1232g
8. Pol. 216
9. 47 CFR 54.520
10. 24 P.S. 1303.1-A
11. Pol. 249
13. Pol. 814
14. 18 U.S.C. 2256
15. 18 Pa. C.S.A. 6312
16. 18 Pa. C.S.A. 5903
17. 17 U.S.C. 101 et seq
24 P.S. 4601 et seq
18 Pa. C.S.A. 7611
Pol. 103
Pol. 103.1
Pol. 104
Pol. 218.2
Pol. 220
Pol. 226
Pol. 237

Adopted
April 20, 2010

Last Revised
April 17, 2012

Purpose

The Board supports the use of the Internet and other technological resources in the district's instructional program in order to facilitate learning and teaching through interpersonal communications, access to information, research, and collaboration. The use of all technological resources shall be consistent with the

curriculum adopted by the Board as well as the varied instructional needs, learning styles, abilities, and developmental levels of the students.

Definitions

This policy addresses the use of all **district systems**, which includes, but is not limited to, any district-owned, leased or licensed computers, hardware, software, or other technology, including the district network, district programs, or district data (including images, files, electronic communications, and other information) attached or connected to, installed in, or otherwise used in connection with a computer.

Computer includes, but is not limited to, any desktops, notebooks, powerbooks, tablet PCs, laptops, printers, cables, modems, telephones, peripherals, specialized electronic equipment used for students' special educational purposes, global positioning system equipment, personal digital assistants, cell phones, cameras, video cameras, beepers, two-way radios, laser pointers, handheld video game systems, iPods, MP3 players, CD players, white boards, DVD players, and Blu-ray players.

This policy also applies to any device owned by any person that is used to access the district network, any district system, or any district-owned, leased, or licensed computer.

Access to the Internet - a computer shall be considered to have access to the Internet if the computer is equipped with a modem or is connected to a network that has access to the Internet, whether by wire, wireless, cable, or any other means.

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]

Harmful to minors - under federal law, is any picture, image, graphic image file or other visual depiction that:[2][3]

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.

Inappropriate matter - any material that, in addition to items defined under "harmful to minors," constitutes a safety/security concern, creates a hostile or intimidating environment, or violates any existing district policy or the Code of Student Conduct.[3]

Incidental personal use - use of district systems by an individual employee for occasional personal communications is permitted. Personal use must comply with this policy and all other district policies, procedures and rules, as well as Internet Service Provider (ISP), local, state and federal laws and may not interfere with the employee's job duties and performance, with system operations, or with other system users, and must not damage the district's systems. Under no circumstances should the employee believe his/her use is private. The district reserves the right to monitor, track, access, and log the use of its systems at any time.

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, storage media, software, and other computers and/or networks to which the district network may be connected, such as the Internet, the Internet2, or those of other institutions.

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.[3]

User - any student, staff or guest who accesses any district network resources or facilities, including but not limited to, district computers, the district network, district hardware, district software, accesses the Internet through the district's connection, or any other district systems.

Vandalism - any malicious attempt to harm or destroy the district's computers, data, applications, and/or network functionality or the data, applications, or functionality of another user's computer. This includes, but is not limited to, the uploading or creation of computer viruses.

Authority

Internet access, electronic mail (email) and network resources are available to staff and students in the district for educational and instructional purposes and other purposes consistent with the educational mission of Bedford Area School District (BASD). The Board establishes that use of the Internet, district email, and all other district systems is a privilege, not a right. Inappropriate, unauthorized, and illegal use will result in cancellation of those privileges and appropriate disciplinary action.[4][5][6]

This Board policy is provided so technology users are aware of their responsibilities when using the BASD's technology resources and to explain to users that they will be held accountable for their noncompliance with this policy. The district's technology resources are made available to users to support district educational goals by facilitating resource sharing, innovation, and communication among faculty, students, administrators, and the community.

The BASD provides network access within all buildings. District technology access and related resources are provided for the purposes of authorized academic and instructional activities, research relating to curricular topics, district communications, and administrative needs. The network and its connections to other networks are to be used only in a manner that is consistent with these purposes and within the spirit of this policy.

The district does not endorse or approve any content accessible through the use of the network facilities, nor does the district guarantee the accuracy of information received on the Internet. Users assume responsibility for any damages suffered as a result of information obtained through the district's systems. The user is solely responsible for any claims, lawsuits, causes of action, damages, judgments, losses, expenses, and liabilities arising from their actions while using the district's systems, without limitation.

Under no circumstances shall there be any expectation of privacy when using any district systems or computers. 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 and shall exercise its right to inspect and examine any use of the district systems or computers; this includes, but is not limited to, a user's Internet access, email transmissions, and all system registries. To ensure reasonable, efficient, and safe use of technology resources, the BASD Technology Department periodically monitors the systems and the accounts used by students, employees, and the visiting community members. The district also reserves the right to access any user accounts or files at any time, for any reason.

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. Traffic originating from any and all such nonauthenticating nodes within the network must not be transmitted from the network, into or through the network.

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. The district is not responsible for restoring any personally installed applications or data which may have been lost or damaged when using the network. The district reserves the right to reimage any district computer at its discretion. The district also reserves the right to examine the contents of any district-owned computer at its discretion and without notice. Hard drive space for storage of personal files is limited; users are encouraged to delete any inactive files that might have been stored on network servers. To ensure deletion of inactive files, the Technology Department will periodically purge these files. If possible, advance notice will be given before purges occur. The Bedford Area School District makes no guarantees regarding the storage of personal files.

Use of the District Network and District-Owned Equipment

The BASD network and technology resources are maintained for the use of students, employees, and the visiting community. Network access is restricted to those with active accounts issued by the BASD Technology Department. User access to BASD technology resources is a privilege, not a right. Accounts may be

revoked, suspended, or modified at any time by district administration as a result of a violation of this policy or any other district policy, where appropriate, as determined in the sole discretion of the district administration.

The use of personal computing devices on the BASD network is permitted only on specially designated networks. When a student, parent/guardian, or employee connects a personal computing device (including but not limited to laptops, flash drives, and cell phones) to a BASD-operated network, they are agreeing to the requirements contained in this policy and should consider his/her personal device subject to the same levels of monitoring and access as any BASD-owned, leased, or licensed technology device. These devices, once in a district building, may not be allowed to connect to an outside network in an attempt to circumvent district-owned filtering hardware or software. All members of the BASD community shall be offered free and appropriate access to technology services to either meaningfully participate in the education program and/or fulfill their job-related responsibilities.

Personal Information and Security

The BASD uses various third party websites for instructional purposes. Many of these websites (commonly referred to as Web 2.0 tools) collect limited amounts of personal data. While the district will make every effort to limit the amount of data disclosed, some items, such as first name, last name, username, and password are required for use of these websites.

The BASD cannot make any guarantee that these websites will protect the data submitted to them. The BASD abides by the Family Educational Rights and Privacy Act and does not disclose any information such as grades or attendance to these websites. Students and staff should not expect any privacy or data protection when using these websites.[7][8]

To comply with the Children's Internet Protection Act of 2001, content and message filters prevent students from sending and receiving email from unauthorized addresses. External email addresses are only permitted to communicate with student accounts if they are related to a specific instructional project.

Bedford Area School District believes in treating its students, parents/guardians, and employees with respect and in turn expects them to treat one another in the same manner. However, students, parents/guardians, and employees must be aware that all information assets (computers and the information that users might store on them) belong to the Bedford Area School District. The BASD has the right to gain access to any of those assets at any time, for any reasons. Students, BASD employees, and the visiting community have no expectation of privacy with respect to any information that they create, store, or otherwise access using BASD technology resources. Network administrators may review student and staff files and communications to maintain system integrity and to ensure that students and staff are using the system only for appropriate purposes. Users should expect that files stored on district servers or computers will not be private.

The intent of this policy is to clarify by example the guidelines that apply to determining whether a given use is acceptable or not. These guidelines are not intended to be exhaustive. The final authority for determining whether or not a use is acceptable is the BASD Board of Directors under the advisement of the Superintendent.

Delegation of Responsibility

User Responsibilities

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 other users in both the district and on the Internet.

The building administrator shall have the authority to make determinations regarding whether a particular use is appropriate or inappropriate in accordance with this policy.

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:[2][3][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 provided instruction at every grade level on network etiquette and other appropriate online behavior, including:[3]

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

2. Cyberbullying awareness and response.[10][11]

Access

Users are given their own personal I.D. Computer account passwords are and should always remain confidential. Providing a user name and password to anyone, or assisting someone to gain unauthorized access to the BASD network is strictly prohibited. Use of another person's identity, account, user name, or password or otherwise gaining unauthorized access to computing or network resources is also strictly prohibited. Users are also expected to immediately report any security breach or corruption of data or electronic files to an administrator. Users are responsible for their individual accounts and should take reasonable precautions to prevent others from using their account. Users must log off or lock the computer when finished or when leaving their work station.

Misuses of passwords, unauthorized copying of another's work, and attempting to access files maintained by others is strictly forbidden.

Personal files should not be saved on the network and may be examined by the district at any time.

Guest accounts may be acquired and must be used solely in compliance with the authorization granted by the administration and the limitations placed upon this access by this policy and any administrative directives. Guest accounts used in violation of this policy shall be subject to all disciplinary measures available through this policy.

The administration reserves the right to limit the level of access as determined in its sole discretion based upon the user's job requirements and needs.

When a user is no longer a student, employee, or guest of the district, their account will be deleted or suspended. Special circumstances may be approved by the Superintendent to allow accounts to continue to be maintained for a defined period of time.

Prohibited Activities

The list below was crafted to convey a sense of the types of activities that are allowed and not allowed, giving some reasons where appropriate. It is not to be considered an exhaustive list of all prohibited activities:

1. Security on a computer system that involves many users is a high priority. To protect users from unwanted contact or harassment, BASD community members are instructed not to give out any personal information pertaining to themselves, the school, or others to anyone. Users shall not distribute or publish any password, identifying code, personal identification number, user name, or any other confidential information about a computer, computer system, network, or email account or database.

2. Impersonation and anonymity are not permitted. Users must take responsibility for their actions and words. Use of a pseudonym or impersonation of another person in any setting, including online, is not permitted. The use of anonymous proxies is considered impersonation and

is strictly forbidden. Proxy usage will result in immediate account revocation and disciplinary action.

3. Facilitation of any illegal activity.

4. Use which is not school or work related, except for incidental personal use. Email is not to be used for the mass mailing of noneducational or nonwork related information or for the sending of unsolicited commercial electronic mail messages, commonly known as spam.

5. The BASD network exists exclusively to support the BASD's educational mission and to facilitate communications by and between employees, students, parents/guardians, and others consistent with that purpose. Considerate and respectful discourse/discussion is expected of all users. Harassing, insulting, discriminatory or hateful speech, terroristic threats, or the attacking of others is strictly prohibited. Offensive speech of this nature is disrespectful of the rights of others; be polite and professional when composing messages and emails. Any of these activities in violation of this policy and the district's cyberbullying policy will result in disciplinary action to the extent appropriate.[11]

6. At no time shall inappropriate or profane language be permitted.

7. Attempting to or actually accessing, creating, distributing, transmitting, or downloading objectionable material by users is prohibited. Users are prohibited from accessing, creating, transmitting, transferring, or downloading defamatory,inaccurate, abusive, obscene, rude, inflammatory, profane, sexually explicit or otherwise lewd, pornographic, threatening, racially offensive, or illegal material on BASD technology resources.

8. No students, faculty, or guests shall attempt to or actually access, download, create, or transmit any material that is harmful to minors or is determined to be inappropriate for minors in accordance with Board policy.

9. Users are expected to adhere to copyright laws. Transfer or use of copyrighted material without a license or proper authorization is a violation of federal law and, therefore, strictly prohibited, and is described in more detail later in this policy.

10. Software and electronic files that have not been selected and installed by the Technology Department can potentially cause a variety of problems when introduced to BASD technology resources. Furthermore, the licensing terms of software programs may not permit their use on the BASD network. For these reasons and to facilitate the general integrity of the network and computing environment, the installation, storage, or running of software programs, applications, utilities, and other electronic files not explicitly authorized by the Superintendent is strictly prohibited. Students will not download files unless instructed to do so by a teacher

who has obtained authorization from the Superintendent or his/her designee. No employee or guest user shall download files unless given explicit permission from the Superintendent or his/her designee.

11. Loading or using unauthorized games, program files, music, or any other electronic media, pirated software, and peer-to-peer file sharing software is strictly prohibited.

12. No user shall engage in any activity which disrupts the work of other users.

13. No user shall quote the personal communications of another user in a public forum without the original author's consent.

14. All computing devices must remain consistent and stable. Users are prohibited from changing settings or adding software to computers unless the Technology Department otherwise authorizes them to do so.

15. No users shall transmit confidential information about students, employees, or district operations without administrative authority.

16. Accessing social networking sites for noncurricular purposes, including participation in unauthorized Internet Relay Chats, instant messaging communications and Internet voice communications (online, real-time conversations) that are not for school-related purposes or required for employees to perform their job duties. Under no circumstances should faculty members interact with students on social networking sites.

17. No user shall participate or access any discussion or news groups that cover inappropriate and/or objectionable topics or materials, including those that conform to the definition of inappropriate matter in this policy.

18. No user shall access or transmit any form of gambling, including but not limited to, basketball and football pools, online poker websites, and any other form of betting, gambling, or games of chance.

19. Product advertisement and engaging in activity which is commercial, for-profit, or for any other business purpose (except where such activities are otherwise permitted or authorized under applicable district policies); conducting unauthorized fundraising or advertising on behalf of the district and nonschool organizations; reselling of district computer resources to individuals or organizations who are not related to the district; or use of the district's name in any unauthorized manner that would reflect negatively on the district, its employees, or students. **Commercial activity** is offering or providing goods or services or purchasing goods or services for personal use. District acquisition policies will be followed for district purchase of goods or supplies through the district system.

20. As a federally tax-exempt, nonprofit organization, the BASD is prohibited from participating in any campaign activity for or against political candidates or any lobbying activities. Therefore, any use of the BASD technology resources for such activities is prohibited, including links to other Internet sites from the BASD Intranet or external Internet site.

21. No user may access, interfere with, possess, or distribute confidential or private information without permission from the district administration, e.g., accessing another student's account to obtain their grades. Users may not violate the privacy or security of electronic information contained on the network.

22. Network bandwidth is a shared resource intended primarily for academic and administrative uses. Excessive downloading or streaming of nonacademic material may result in the elimination of such services at the discretion of district administration.

23. All BASD students, faculty, staff, and visiting community members are expected to use technology resources in a professional and appropriate manner. Exemplary behavior is expected on "virtual" field trips, collaborative videoconferences, and when visiting locations on the Internet. Use of the Internet is intended for the completion of academic work and legitimate BASD-related business.

24. Proper electronic communication etiquette is expected of all users. The creation, sending, or forwarding of email chain letters, inappropriate or unprofessional content is prohibited. The BASD email distribution lists are for school business only, never for personal or commercial purposes.

25. Computer Game Playing – users may not use BASD computers for game playing unless for a specific purpose in a course or faculty supervised club or grade level activity.

Violation of any of the above provisions in this policy may result in the suspension, termination of a user's privilege to technology resources and/or a restriction of the user's privileges. All users should understand that if they commit any violation of this policy, their access privileges may be suspended or revoked, school disciplinary action will be taken, and/or appropriate legal action may be instituted.

Materials stored on individual computers and fileservers are the property of the educational agency and are, therefore, accessible by the educational agency at any time and can be disclosed to whomever the agency desires at any time. Electronic files and communication are subject to disclosure as deemed necessary to maintain compliance.

Operational Prohibitions

The following operational activities and behaviors are prohibited:

1. Interference with or disruption of the district systems, network accounts, services, or equipment through, but not limited to, the propagation of computer worms and viruses; Trojan horse and trapdoor program code; the sending of electronic chain mail; distasteful jokes; and the inappropriate sending of broadcast messages to large numbers of individuals or hosts.

2. The user may not hack or crack the network or others' computers, whether by parasiteware or spyware designed to steal information; viruses; worms; other hardware or software designed to damage district systems, or any component of the network; to strip or harvest information; to completely take over a person's computer; or to allow the intruder to "look around."

3. Tampering with network hardware or software.

4. Gaining unauthorized access into other protected areas of the network.

5. Attempting to or actually bypassing the district's filtering software.

6. Intentionally vandalizing or destroying network files or data belonging to or used by others, or other behavior that interferes with the function of the district network.

7. Altering or attempting to alter files, system security software, or any district systems without authorization.

8. Unauthorized scanning of the district systems for security vulnerabilities.

9. Attempting to alter any district computing or networking components (including but not limited to fileservers, bridges, routers, or hubs) without authorization or beyond one's level of authorization.

10. Unauthorized wiring, including attempts to create unauthorized network connections, or any unauthorized extension or retransmission of any computer, electronic communications system, or network services, whether wired, wireless, cable, or by other means.

11. Connecting unauthorized hardware and devices to the district systems.

12. Loading, downloading, or use of unauthorized software, games, programs, files, or other electronic media, including but not limited to downloading music files, pirated software, and peer-to-peer file sharing software.

Any user who violates the prohibitions of this section will be strictly liable for any damage to district systems without regard to intent to cause harm. The action taken in violation of this section of the policy shall be sufficient to establish the individual's intent to cause harm.

Disclaimer

The Bedford Area School District makes no warranties of any kind, whether express or implied, for the service it is providing. The district is not responsible and will not be responsible for any damages, including loss of data resulting from delays, nondeliveries, missed deliveries, or service interruption. Use of any information obtained through the district's computers is at the user's risk. The district disclaims responsibility for the accuracy or quality of information obtained through the Internet or email.

Other Communications

Other communications include but are not limited to: email, chat rooms, discussion boards, blogging, instant messages, journaling, or any other communication tool.

Users may be granted district email accounts for work-related and incidental personal use.

Incidental personal use of school computers is permitted as long as such use does not interfere with the user's job duties and performance, with the system operations, or other system users. **Incidental personal use** is defined in this policy and includes use by an individual employee for occasional personal communications. Users are reminded that such personal use must comply with this policy and all other applicable policies and procedures. Further, even incidental personal use is subject to district oversight and review at any time.

Electronic communication is subject to district review at any time. No electronic communication sent through the district system is private. Under certain circumstances, such as a result of investigations, subpoenas, or lawsuits, the district may be required by law to disclose the contents of electronic communications to a third party.

Access to email programs or web-based email providers, other than the approved district email program, is prohibited on the district systems. All school-related correspondence must be sent via the email account provided by the district.

Other types of communication programs are to be used for educational purposes only and must be connected to the curriculum. All communication programs which the faculty wishes to use for educational purposes must be reviewed and approved by the Superintendent or his/her designee.

Due Process

The district will cooperate with the district's ISP, local, state, and federal officials to the extent legally required in investigations concerning or relating to any illegal activities conducted through the district's systems.

If students or employees possess due process rights for discipline resulting from the violation of this policy, they will be provided such rights in accordance with the law.[4][5][6]

The district may terminate the account privileges of any user without prior notice.

Search and Seizure

Violations of this policy, any other district policy, or the law may be discovered by routine maintenance and monitoring of the district system, or any method stated in this policy, or pursuant to any legal means.

The district reserves the right to monitor, track, log, and access any electronic communications, including but not limited to, Internet access and emails, at any time, for any reason. Users have no expectation of privacy in their use of the district systems and technology, even when used for incidental personal reasons. Further, the district has reserved the right to access any personal technology device of users brought onto the district's premises or at district events, connected to the district network, containing district programs, or containing student data in order to ensure compliance with this policy and other district policies, to protect the district's resources, and to comply with all applicable laws.

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 are not to use a computer that has been logged in under another student's or teacher'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.

4. The district's Technology Department has the authority to request a user's passwords for troubleshooting or any other technical services.

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 immediately shall bring them to the attention of a teacher or administrator.

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

Network users shall not reveal personal addresses or telephone numbers to other users on the network. Student users will not agree to meet with someone they met online while using district systems.

Internet safety measures shall effectively address the following:[3][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.

Consequences for Inappropriate Use

The network user shall be responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts. Deliberate and willful acts will be construed so as to include any accidental infection or other harm resulting from the intentional violations of any provision of this policy, even if infliction of the infection or other harm was not the intended goal of the activity.

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.

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.

As stated in other sections of this policy, access to the Internet and district systems and technology is a privilege, not a right; and inappropriate, unauthorized, and/or illegal use will result in the cancellation of access privileges and appropriate disciplinary/legal action.
Any act of vandalism will be subject to an appropriate penalty as provided for herein without regard to the user's intent or purpose in carrying out the prohibited activity. The district reserves the right to prosecute and hold liable any user whose activities in violation of this policy or acts of vandalism result in damage to the district's systems. Users whose actions inflict damage upon the district's systems shall be held liable for any damages resulting from their acts in violation of this policy.

Vandalism will result in the immediate cancellation of access privileges and the district reserves the right to prosecute and hold the user liable for any damages, foreseen or unforeseen, resulting from the user's acts of vandalism.

Under Pennsylvania law, it is a crime to access, alter, or damage any computer system, network, software, or database, or any part thereof, with the intent to interrupt the normal functioning of an organization. It is also unlawful to knowingly and without authorization disclose a password to any computer system or network, to gain unauthorized access to a computer or to interfere with the operation of a computer, or to alter any computer software without authorization. Violations of these sections of Pennsylvania law are a felony punishable by a fine of up to $15,000 and up to seven (7) years of imprisonment. Disclosure of a password to a computer system or network knowingly and without authorization is a misdemeanor punishable by a fine up to $10,000 and imprisonment of up to five (5) years.
Users are placed on notice that their actions in violation of this policy and any applicable law, can and will, where appropriate, result in criminal and/or civil prosecution.

Copyright

Federal laws, cases, and guidelines pertaining to copyright will govern the use of material accessed through the district resources. 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 guidelines. All users must comply with the mandates of copyright law and shall not use copyrighted materials illegally or without a proper license, nor shall any user commit an act of plagiarism. The illegal use of copyrighted materials is strictly prohibited. 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 will comply with license agreements.[13][17]

Violations of copyright law may be a felony and the law allows a court to hold individuals personally responsible for copyright infringement. The district does not, and will not, tolerate violations of federal copyright law. Therefore, any user violating federal copyright law does so at their own risk and assumes all liability for their actions.

Violations of copyright law include, but are not limited to, the making of unauthorized copies of any copyrighted material, 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, shrinkwrap, clickwrap, browsewrap, and electronic software downloaded from the Internet.

District guidelines regarding plagiarism will govern the use of material accessed through the district systems. Users will not plagiarize works that they find and

acts of plagiarism are strictly prohibited and will be subject to appropriate punishment. Teachers will instruct students in appropriate research and citation practices.