No. 814.1
OPERATIONS
ACCEPTABLE USE OF NETWORKS
ADOPTED: MARCH 24, 1997
REVISED: NOVEMBER 25, 2013

814.1 ACCEPTABLE USE OF NETWORKS, INTERNET AND COMPUTING RESOURCES

Terms of Agreement

The Millville Area School Board requires all users (administrators, teachers, support staff, students and guests) of the District's computers, networks, and Internet access to read and accept terms set forth in the Acceptable Use of Networks, Internet and Computing Resources Policy before signing the Acceptable Use Agreement. Failure to comply with the terms of this agreement could result in the cancellation of the user's account and/or computer usage privileges. Students will also need signed parental permission to use the Internet.

Purpose

The Millville Area School Board supports the 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 communication and access to information, research and collaboration. For educational purposes, the use of the network facilities shall be consistent with the curriculum adopted by the School Board as well as the varied instructional needs, learning styles, abilities, and developmental levels of students. The term educational purpose includes use of the system for classroom activities, professional or career development, limited high-quality self-discovery activities, and administrative applications.

For operational purposes, network facilities shall be used to increase productivity, enhance communication, provide access to information, and for research and collaboration on district initiatives in a variety of operational areas. District resources may not be utilized for personal endeavors or for entertainment purposes during the scheduled work day.

This Acceptable Use Policy does not attempt to address every required or prohibited behavior by its users. Therefore all users must conduct themselves in a responsible and ethical manner at all times. The user is ultimately responsible for his or her behavior and actions when using technology.

This Acceptable Use Policy applies to all students, employees and visitors.

Authority

The electronic information available to students and staff does not imply endorsement by the School Board of the content, nor does the Board guarantee the accuracy of information received. The School Board 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. Users are responsible to back up personal documents. The School Board shall not be responsible for any unauthorized charges or fees resulting from the Internet.

The right is reserved to log network use and to monitor and restrict storage space and bandwidth utilization by District users, while respecting the privacy rights of both District users and outside users. Inappropriate, unauthorized and illegal use will result in cancellation of those privileges and appropriate disciplinary action.

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 school district. Use of the system is governed by this policy. Users shall have no expectations 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 and Internet browsing history. The district reserves the right to monitor, track and log network access and use; monitor fileserver utilization; 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, local, state, and federal officials in any investigation concerning or related to the misuse of the district's Internet, computers and network resources.

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, including teachers, principals, or Technology staff.

General Computer Usage

The Millville Area School Board recognizes the role of information and technology in the academic community and in the large society. It is the policy of the School Board to provide all students, faculty, and staff with access to a variety of technology resources and to provide opportunities for all members of the District community to learn to utilize these resources effectively and efficiently. In return, it is expected that technology usage will be conducted in legally and ethically appropriate ways. All technology resources will be used in accordance with established policies of the School Board and with any and all local, state, and federal laws, and/or guidelines governing the use of technology and its component parts. Implicit in this is the expectation that all students, faculty, and staff will utilize the technology resources of the District so as not to waste them, abuse them, or interfere with or cause harm to other individuals, institutions, or companies. Users are expected to balance their own needs against the needs and expectations of other users.

Accounts

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

Guest accounts may be considered for non-district staff or students if there is a specific, district-related purpose requiring such access. Use of the system by a guest must be specifically limited to the district-related purpose. An agreement may be required.

Equipment

Each employee or student who is issued a laptop, i Pad or other technology, shall be responsible for the security and care of the hardware, regardless of whether it is used in the district or outside the district.

Users shall be responsible for all content on their district issued device. All district computer, laptop, and i Pad content may be monitored at any time by the district.

Software and Hardware

1. School District computers are configured and maintained for educational and administrative purposes only and should not be viewed as the personal equipment of the user. Therefore, the right is reserved to restrict the configuration and installation of software and hardware on all district computers.

2. Any software installed on District computers must be licensed in accordance with the law. A separate license must be purchased for each computer upon which the software is installed. A copy of all licenses must be forwarded to the Technology Department staff before installation.

3. Users may not make unauthorized copies of software that is copyrighted.

4. Users may not install any unauthorized games, programs, files, or other electronic media on District computers.

5. Users may not move or remove equipment or install hardware or software without authorization by the Technology Department staff.

6. Users may not attempt to repair hardware or purchase component parts without authorization by the Technology Department staff.

7. Users will allow authorized technicians access to District computers for purposes of repair or installation.

8. Users may not physically damage or destroy hardware or do so by the introduction of worms or viruses. Vandalism, including theft of computer components, will result in monetary damages paid by the perpetrator, as well as disciplinary action according to District policy.

System Security

1. Users may not modify technology resources, utilities, and/or configurations, or change the restrictions associated with their accounts, or attempt to breach any technology resources security system, whether with or without malicious intent.

2. Users may not attempt to crash a system, or exploit weaknesses in security. If weaknesses are found by students, they must be reported immediately to the classroom teacher. District employees must report security weaknesses to the Technology Department staff as soon as possible but no later than one working day from the time of the discovery.

3. Users must immediately notify the Technology Department staff if they have identified a possible security problem or possible virus intrusion. Users may not search for security problems; this may be construed as an illegal attempt to gain access.

4. Users may not engage in malicious hacking, i.e. deliberately breaking into a system to alter or damage it or for the purpose of getting illegitimate access to resources or information.

5. Users may not misuse technology resources in any way that materially impacts on the desired result of others.

6. While using the District network, users will not disseminate or archive on District network resources or those external to the Millville Area School District network any identifying criteria about other users.

7. Users are responsible for the use of their individual account and should take all reasonable precautions to prevent others from being able to use their account, including logging off when away from the computer, especially if the computer is in an educational or insecure workplace setting. Unless authorized, users should not provide their password to another person. Certain networked software applications may require the use of a user's password by a substitute who has been hired and needs to perform the same tasks as the absent employee.

8. Users may not use a computer that has been logged in under another student or employee's name.

9. Users may not give others access (via password or other means) to computing resources to which they are not entitled.

10. Users may not use someone else's password or log in to someone else's account without authorization, except as may be required for management of system resources.

11. Users may not attempt to gain access to computing privileges or resources for which they are not authorized or via means not authorized.

12. Users may not use the system in any way to impersonate another user or to hide their identity through the use of pseudonyms or anonymity.

13. Administrative or office computers should be utilized for their intended functions and should not be available to other users for general or personal use.

14. Users may not read, execute, modify, or delete any file belonging to someone else without explicit permission from the owner, even if the file is unprotected.

15. Users may not use a system for unauthorized purposes such as advertising for a commercial organization, running a business, political lobbying, or illegal activities.

16. Users may not create, display or transmit obscene, libelous, or threatening messages or materials on the District's computer equipment.

17. An authorized system administrator may remove or alter as necessary user files that threaten to interfere with the operation of the system or as needed for system maintenance such as files infected with a virus, unauthorized programs that have adverse effects to the infrastructure, or copyright infringements. The system administrator should make every effort to notify the user prior to such action to give the user opportunity to remove such files him/herself. It is recognized that there may be special cases where the threat to the effectiveness of system resources is so immediate that prior notification is not possible. Users should keep backup copies of critical files.

18. System users should have no privacy expectation in the contents of their personal files on the district system. Users should be aware that their personal files are discoverable under state public records laws and may be accessed or intercepted at any time.

19. The use of personal (non-district) devices on the network will not be supported. Personal devices should be registered in the building office with appropriate serial numbers and ownership information. The District is not liable for any damage done to personal devices. District-owned components may not be installed in a personal device. Devices include, but are not limited to phones, Kindles, or other Wi-Fi capable electronics.

20. Users may not create, implement, or host their own servers or services using District resources, unless part of approved District curriculum/coursework.

21. Excess e-mail or files taking up an inordinate amount of fileserver disk space may be removed by system administrators, after a reasonable time and notification to the user.

Acceptable Use of the Internet

System Security

1. A commercial software filter has been implemented that blocks access for minors and adults on the Internet to web sites with visual depictions and text that are obscene, contain child pornography, are harmful to minors with respect to use by minors, or that are determined inappropriate for use by minors by the School Board. No guarantees are made that the filters will block 100% of the offensive material 100% of the time. No filtering system is 100% effective, partially due to the vastness and volatility of the Internet, and partially because of the arbitrary nature of the categorization. The same filters will apply to elementary and secondary students and to the staff. Accessing inappropriate material will be considered an unacceptable use of school resources and will result in suspension of Network privileges and/or disciplinary action as outlined in appropriate District policies.

2. An Internet usage log will be maintained and secured. Online activities of users may be monitored.

3. Students are prohibited from unauthorized disclosure or dissemination of personal identification, including but not limited to the student's first or last name, address, phone number, picture, or email address.

4. District employees are prohibited from the unauthorized disclosure or dissemination of information about students' records, including but not limited to the student's first or last name, address, phone number, picture or email address.

5. Routine maintenance and monitoring of the system may lead to discovery that the user has or is violating the District Acceptable Use Policy, the discipline policy, or the law.

6. An individual search may be conducted if there is reasonable suspicion that a user has violated the law or the District policies. The nature of the investigation will be reasonable and in the context of the nature of the alleged violation.

Inappropriate Access to Material

1. Users may not use, attempt to use, or direct the use of the District Internet system to access material that is profane or obscene (pornography), that advocates illegal acts, or that advocates violence or discrimination towards other people (hate literature). A special exception may be made if the purpose for accessing hate literature is to conduct research and has teacher and parent approval.

2. If a user inadvertently accesses such information, he or she must immediately disclose the inadvertent access in a manner specified by his or her teacher or building administrator. This will protect users against an allegation that they have intentionally violated the Acceptable Use Policy.

Cell Phones and Personal Electronic Devices

1. Cell phones and personal electronic devices, including but not limited to, mp3 players, gaming devices, tablet computers, and personal laptops are permitted on campus, but are not to be used during class time, unless authorized by school officials. The above will not and shall not be attempted to be connected to the district network in any way.

2. Students are not permitted to send or take photographs or videos with their electronic device on school property or at school events unless authorized by school officials.

3. The district is not responsible for the safe keeping or content of these devices.

4. Misuse of such devices may result in confiscation and/or applicable punishment according to district policy and rules.

Cameras and Webcams

1. Cameras, recording devices or similar capturing devices are not allowed on campus, unless authorized by school officials.

2. Web cams are provided standard on some district owned computers and devices.

Social Networking and Websites

1. Social networking sites, including, but not limited to, Facebook, shall not be accessed during school hours on either district or personally owned computers and devices, unless under direct supervision and with approval of classroom teacher or school official.

2. Students are not permitted to access any photograph sharing websites from district technology.

3. Students are not permitted to access any dating or rating websites from the district technology.

Instant Messaging

1. Students are not permitted to access any instant messenger services.

Blogging

1. If an employee, student, or guest engages in blogging sites, the user must not violate any privacy rights of another user. Users may not use distinct personal or private data, images or copyrighted material in their blog. Misconduct will result in disciplinary actions expressed under the Actions Resulting from Policy Violations section.

Email

1. District employees and students may be provided with a district email account to use for educational purposes or district-related business.

2. Users will not use email for personal advertisements or to forward jokes, chain letters, or other mass mailings that are not school-related or appear to be spam.

3. Users may not repost a message that was sent to them privately without the permission of the person who sent them the message.

4. Users may not post private information about another person.

5. Users may not knowingly or recklessly post false or defamatory information about a person or organization.

6. Users may not post any inappropriate material or material that could be construed as harassment or bullying/cyber bullying.

7. Users may not post any inappropriate material or material that could be construed as harassment or bullying/cyber bullying.

8. Users may not use vulgar, abusive profane or other offensive language on District email.

9. Users may not discuss illegal activities on District email or use the district system to engage in any other illegal act, such as arranging for drug sale or the purchase of alcohol, engaging in criminal gang activity, threatening the safety of person or property, etc.

10. Users may not send attachments that are not school-related.

11. Email may be subpoenaed by authorities in the incidence of any legal action taken upon an individual.

12. The district respects students and staff members and values their privacy. However, in order to maintain system security, users should have no privacy expectation in their e-mail messages. The District may intercept or access stored communication at any time for any reason.

13. Students may be assigned an email account based on curriculum or college and career readiness needs, such as email for college applications.

14. Students are only permitted to use district provided email accounts.

Commercial Purposes

1. Users may not use the District Internet system for commercial purposes. Commercial purposes are defined as offering or providing goods or services for personal use. District acquisition policies will apply to the District purchase of goods or services through the system.

Copyright Issues

1. Copyright laws will govern the use of material accessed through the District system. Users that violate copyright laws will be solely liable for such violations.

2. Users may not use or install unlicensed software on District computers.

3. Users may not violate the law by illegally duplicating software.

4. Users may not plagiarize. Teachers will instruct students in appropriate research and citation practices.

5. When using material (text, graphics, sounds, movies) from the Internet which could not be considered Fair Use of educational purposes, the user must request permission from the creator of the material before duplicating said material in any way. All materials on the Internet are copyrighted, whether so stated or not.

6. Users may not download materials in any format that are copyrighted without permission from the copyright holder, unless it is so stated that the material is free to download and use.

Establishment of Web Sites

1. The District Web site has been established to develop Web pages that present information about the District. The Technology Coordinator or his/her designee will be responsible for the creation of, maintenance of, and posting to the Web site. All Web pages will be posted at the discretion of and by the Technology Coordinator or his/her designee, unless otherwise stipulated by the Technology Coordinator, Superintendent, or the Board.

2. District employees may not officially or unofficially represent the School District on non-District Web sites. The Millville Area School District is not liable for information posted on a non-District site.

3. Groups associated with the School District such as PTO's, booster clubs, band associations or other associations representing School District activities, may not establish web sites representing any School District affiliated group without review by the Technology Coordinator of all material to be posted before it is posted.

4. Schools and classes may establish Web pages that present information about the school or class activities or for educational purposes. Teachers are responsible for the content created by their students. Student-created web pages will be posted at the discretion of and by the Technology Coordinator or his/her designee. Disclaimers may be required stating that "Opinions expressed on this web page shall not be attributed to the Millville Area School District."

5. With the approval of the Technology Coordinator, extracurricular organizations may establish Web pages. Advisors to the activities will be responsible for the content. Material presented on the organization Web page must relate specifically to organizational activities. Disclaimers may be required, stating that "Opinions expressed on this page shall not be attributed to the Millville Area School District." The Technology Coordinator or his/her designee will post organizational Web pages, unless otherwise stipulated by the Technology Coordinator, Superintendent, or the Board.

6. Any links occurring on District Web pages must be done in accordance with the law and must be linked to sites that have an educational purpose. No links may occur within frames. The linked Web site must be identified due to copyright considerations. Links may not be identified with defamatory, slanderous, libelous, or inappropriate language. No attempt should be made to misrepresent the location of a link. When links are used on a District Web page, a reference must be made that states that "The Millville Area School District is not responsible for information contained on linked sites."

7. Users will not have access to posting information on the authorized District Web sites, unless otherwise stipulated by the Technology Coordinator.

8. The Technology Coordinator reserves the right to edit or remove any material posted to any of the authorized District Web sites.

9. Advertising for commercial, political, or religious purposes is prohibited on District Web pages.

10. Threats or intimidating statements made in reference to persons within or outside the District are prohibited from being posted on any District website or resource.

Student Records

1. Student directories will not be published on District Websites.

Content Guidelines

Information saved to the district network or website shall abide by the following guidelines:

1. Shall not include student's private information such as birthdate, social security number, address, phone numbers, family member names, etc.
2. Shall not include personally identifiable information indicating a student's location without parental consent.
3. Shall not contain or link to objectionable material.
4. Must conform to all district policies.
5. Any content created with school technologies will be considered property of the school district.

Freedom of Speech When Using District Resources

1. Students have the right to exercise freedom of speech, including the right of expression. Disclaimers may be required stating that "Opinions expressed on this web page shall not be attributed to the Millville Area School District."
2. Threats or intimidating statements made with reference to any persons within or without the School District are prohibited from being posted on any District Web site or resource.
3. The expression, publication, or distribution of obscene, libelous or slanderous materials, or materials which encourage students to commit unlawful acts, violate lawful School District regulations, or cause material and substantial disruption of the orderly operation of the School District, are prohibited.
4. Users may not use the District Web site as a forum for criticism of School District policies.

Network Etiquette

1. Users will communicate in a courteous manner when dealing with other users on the network and with regard to any problems encountered when using District resources.
2. Users will not swear, use vulgarities or any other inappropriate language.
3. Users will not reveal their personal address, Network password or telephone numbers of students or colleagues.
4. Users recognize that electronic mail and Network folders are not guaranteed to be private. Building and system administrators reserve the right to review all system content.

Political Activities

1. Users may not use the District system for political lobbying.

Illegal Activities

1. Users may not use the District system to engage in any illegal activities. Such activity is strictly forbidden and may be reported to authorities.

Selection of Materials

1. When using the Internet for class activities, teachers will select material that is appropriate for the age of the students and that is relevant to the course objectives. Teachers will preview the materials and sites they require. Teachers will provide guidelines and lists of resources to assist their students in their research activities. Teachers will assist their students in developing the skills to ascertain the truthfulness of information and to distinguish fact from opinion.

2. Internet downloads will be restricted to those files that have an educational purpose within the guidelines of the curriculum or in accordance with the requirements of one's job position.

Actions Resulting from Policy Violations

1. Deliberate and/or negligent abuse of the network, computing resources, or any other policy violations as defined herein could lead to disciplinary action as established by the School Board and/or loss of network and/or Internet privileges. Loss of network privileges could result in the failure to meet established academic requirements necessary for graduation or promotion. **Employees who violate the Internet Policy as stated herein are subject to disciplinary action as defined in Board Policy 317, 417, and 517.**

   Loss of Internet access could be one of the disciplinary actions, however, this policy incorporates all other relevant District policies, such as but not limited to, the student and professional employee discipline, copyright, property, website development, bullying, curriculum, sexual harassment and terroristic threat policies. Violations as described in this policy may be reported to the appropriate legal authorities.

2. Offenders may be subjected to criminal prosecution. Under Pennsylvania Law, it is a felony punishable by a fine and imprisonment for any person to access, alter, or damage any computer system, networking, software or database, or any part hereof, with the intent to interrupt the normal functioning of an organization. Disclosing a password to a computer system, network, etc., knowingly and without authorization, is a misdemeanor punishable by a fine and imprisonment, as is intentional and unauthorized access to a computer or alteration of computer software.