BETHLEHEM AREA SCHOOL DISTRICT

Book	Policy Manual
Section	800 Operations
Title	Computer, Network, and Internet Use
Code	815
Status	Active
Legal	1. Pol. 218 2. Pol. 317 3. Pol. 417 4. Pol. 517 5. 20 U.S.C. 1232g 6. 24 P.S. 4604 7. 20 U.S.C. 6777 8. 47 U.S.C. 254 9. Pol. 814 10. 17 U.S.C. 101 et seq 11. Pol. 233 24 P.S. 1303.1-A 18 Pa. C.S.A. 2709 18 Pa. C.S.A. 5903 18 Pa. C.S.A. 6312 24 P.S. 4601 et seq 18 U.S.C. 2256 47 CFR 54.520 Pol. 103 Pol. 104 Pol. 218.2 Pol. 220 Pol. 237 Pol. 249
Adopted	November 15, 2004
Last Revised	October 22, 2018

Purpose

Statement of Objective

The Bethlehem Area School District, in accordance with Board policy, supports the use of the Internet and other technologies 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 district technologies shall be consistent with and enhance the curriculum adopted by the school district and consider the varied instructional needs, learning styles, abilities and developmental levels of students.

Authority

Organizational Responsibility and Privacy

The district establishes that use of the district technology is a privilege, not a right. Inappropriate, unauthorized and/or illegal use may result in cancellation of this privilege and appropriate disciplinary action.[1][2][3][4]

The electronic information available to students and staff does not imply endorsement of the content by the school district, nor does the district guarantee the accuracy of information received from the Internet.

The district shall not be responsible for any information that may be lost, damaged or unavailable when using district technology resources. Backup of such materials shall be the responsibility of the person creating/using them.

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

The district shall not be responsible for any damages incurred by downloading viruses and/or similar invasive technologies from the Internet.

The level of access that employees have to school computers, network and Internet services is based upon specific employee job requirements and needs.

The district attempts to maintain the confidentiality of student records. All users must comply with the Federal Educational Rights and Privacy Act (FERPA).[5]

The school district requires students and staff to sign, manually or electronically, an acknowledgement that they received and read this policy. Users will be provided with copies of any and all amendments and revisions of this policy upon receipt of approval by the district's Board of School Directors.

The school district shall make every effort to ensure that students and staff use this educational resource responsibly.

As required by the Children's Internet Protection Act (CIPA) and the Neighborhood Protection Act, the district has installed filtering software to restrict and monitor the use of the Internet, email, newsgroups, FTP and chat. The filtering software is designed to block or filter Internet access to pictures that are obscene, pornographic, or harmful to minors. However, no filtering software is 100 percent effective. The district reserves the right to disable the filtering software to facilitate specific educational purposes from time to time. Requests to block or unblock a site should be entered as a service desk ticket that will be reviewed and approved or rejected.[6][7][8]

Students and staff have the responsibility to respect and protect the rights of every user in the district and on the Internet. The district believes that it is important to educate students about appropriate online behavior, including cyber bullying awareness and appropriate interaction with other individuals on social networking sites and in chat rooms, and has taken steps to incorporate this information in the appropriate curriculum areas. In addition, all district staff and students are responsible for reading and following this policy.

Users should understand that there is a distinct lack of confidentiality on the Internet. Board policy indicates the email system is for business use only and prohibits any business unrelated to district matters. The policy does recognize that employees may use their email for incidental personal use, but that they can expect no privacy. The policy defines **incidental personal use** as occasional, infrequent personal use that does not impact an employee's duties, does not impact network resources and does not impede educational operations.

Users of district technologies should not have an expectation of privacy in the materials that are created, sent or received by them on district systems. To the extent allowed by laws and regulations, district authorized personnel may examine all material stored on district systems without prior notice.

Messages that are created, sent or received using the district email system are the property of the district. The district reserves the right to access and disclose the contents of all messages created, sent or received using the email system.

Subject to local laws and regulations, the district may monitor any aspects of its computerized resources, including, but not limited to, monitoring sites visited by users on the Internet, monitoring chat groups and newsgroups, reviewing material downloaded or uploaded to the Internet by a district user, reviewing email sent and received by district users and monitoring file server space utilization by district users.

Delegation of Responsibility

Personnel Responsibilities

District personnel are expected to be familiar with the school district's policies and rules concerning student computer and Internet use and to enforce them. It is the responsibility of district personnel to directly supervise students and monitor computers in the use of the Internet and other district technologies. All district personnel who utilize school technology for instructional purposes with students have a professional responsibility to help students develop the skills necessary to identify information sources appropriate to their age and developmental levels and to evaluate the information needed to meet their educational goals. Students are not permitted to utilize computers for non-academic purposes and students are not permitted to use the Internet without direct adult supervision. When, in the course of their duties, personnel become aware of student violations, they are expected to stop the activity immediately and inform their building principal or immediate supervisor.

Guidelines

ACCEPTABLE USE

Network

System security is protected through the use of user-specific passwords. District staff are required to change their password at the district-designated interval. Failure to adequately protect 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. Staff 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 user's name.
3. Users are required to log off of the network when finished.
4. Users must not attempt to obtain or modify files, passwords and data belonging to other users.

5. Users may not use the network in a way that disrupts the work of other users.

6. Users must comply with district network storage limitations.

7. Users are not permitted to store inappropriate materials on any district-designated systems.

8. Users are required to protect and secure electronic information and data from inadvertent disclosure to unauthorized parties. If any user becomes aware of a release of school district information, data, or records, the release must be reported to the Superintendent of Schools or designee immediately.

9. Students may not install or use unauthorized games, applications, files or other electronic media.

10. Vendors who require access to systems for maintenance and updates are required to abide by this policy. Vendors are required to obtain authorization from the Chief Technology Officer before access is granted to systems.

Internet Access

In making decisions regarding student access to the Internet, the district considers its own educational mission, goals and objectives. Electronic information research skills are fundamental to the preparation of future citizens and employees. The district expects that faculty will blend educationally purposeful use of the Internet throughout the curriculum and provide guidance and instruction to students in its proper usage. Students and staff are expected to act in a responsible, ethical and legal manner in accordance with district policy and federal and state law. In addition, all users are required to abide by the terms of our Internet Service Provider's (ISP) Acceptable Use Policy. The contract with our ISP requires compliance with their policy.

Specifically, the following uses of district technology resources are prohibited:

1. Using the network for commercial or for profit purposes.

2. Using the network for product advertisement or political lobbying.

3. Unauthorized or illegal downloading, installation, distribution, reproduction or use of copyrighted materials from the Internet.

4. Accessing, uploading, downloading or distributing pornographic, obscene, or sexually explicit material.

5. Participating in online discussions, blogs and chat room discussions that are not related to the educational mission of the district.

6. Using the network to conduct illegal activities, including but not limited to gambling, cyber bullying, promoting illegal drug use, making terroristic threats or harassment.

7. Using the network in violation of any local, state or federal statute.

8. Loading, downloading or using unauthorized games, programs, files or other electronic media, such as music files.

9. Violating the privacy and security of electronic information.

10. Students may not bypass or attempt to bypass Internet filtering software using anonymizers or proxy servers that mask the content the user is accessing or attempting to access.

11. Disabling or circumventing system security (e.g., virus protection, anti-spam software).

12. Staff and students may use their own personal computers or other devices in accordance with district policy and procedure. However, the district reserves the right to limit bandwidth usage on personal devices.

13. Unauthorized disclosure of students' personal information in email, blogs, instant messages, chat rooms or other Internet communication devices. This includes, but is not limited to full names, addresses, phone numbers, school and activities.

Email

The district expects all users of the district's electronic mail system to follow these policies:

1. Correspond with the understanding that district email is not guaranteed to be private.

2. Do not use district email to send chain letters, jokes, advertisements, items to buy or sell, and other items not related to school business.

3. Users are expected to be polite and professional in the email messages they create and send. Email messages should never be abusive to others.

4. Users are expected to use appropriate language. Inappropriate language, swearing and vulgar comments are prohibited.

5. Email should be used primarily for academic, job-related correspondences, but incidental personal use is permitted.

6. Group email lists are to be used only for communications directly relating to district professional responsibilities.

7. Never impersonate another user, send mail anonymously, or use a pseudonym.

8. Do not open email messages or attachments of unknown origin.

9. All users should check email frequently and remove messages from the server as soon as possible.

10. Email messages sent to the district-wide mailing lists must be district-related in content.

11. When email is used to discuss student issues that fall in the domain of HIPAA, FERPA, or other legal privacy rights, the student's name is not to be used. Instead, the first and last initials of the student are to be used.

12. Communication between staff and students shall be for district-related purposes solely and only district-related accounts should be used for such communication.

Social Networking Media

Social networking media, for the purposes of this policy, refers to any works of user-created video, audio, or multimedia that are published and/or shared electronically. Social networking media include blogs, social networking sites, video hosting sites, instant messaging, electronic video/photo sharing on personal devices, etc.

Recognizing the benefits collaboration brings to education, the district may provide users with access to websites or tools that allow communication, collaboration, sharing, and messaging among users for the purposes of teaching and learning.

The use of personal (not professional) social networking accounts for communication with students is prohibited. If a teacher or other faculty or staff member wishes to use electronic means to communicate directly with students for educational purposes (homework/project reminders or assistance, school-sponsored event reminders, etc.), s/he may utilize an appropriate professional medium, such as professional (not personal) accounts, direct emails from the faculty member's district appointed email address, and/or postings from an educational or district-sponsored, school-sponsored, or team-sponsored tool. Use of such electronic media shall be restricted to appropriate professional uses only.

Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Posts, chats, sharing, and messaging may be monitored. Users should be careful not to share personally-identifying information with others (home addresses, phone numbers, family member names, etc.).

Employee Use of Social Networking Media/Internet Communication/Mobile Device Communication

All communications with students must be of a professional nature. Faculty/Staff members must maintain strict professional boundaries of communication with students. Faculty/Staff members are encouraged not to "friend" students in personal social networking accounts, allow students access to the employee's nonpublic personal pages, or use social networking media to enter into communications with students that are not directly related to instructional matters. The district takes personal/professional boundary limits with students very seriously and will take disciplinary action against any faculty or staff member who violates this policy and/or who initiates or maintains inappropriate personal communications with students. The district recommends that faculty and staff take all necessary steps to limit access to their personal social networking media accounts and prevent students from obtaining such access. Faculty/Staff members are reminded that due to the nature of the technology, individuals do not have an expectation of privacy on social media sites.[2][3][4]

When using any communications media, faculty/staff members may not:

1. Enter into inappropriate communications/relationships with students via any means, electronic or otherwise.

2. Access personal social networking media accounts during the school day or while representing the school at school-sponsored events.

3. Post or share information which students may access that discusses or portrays sex, nudity, alcohol, or drug use or other behaviors associated with the staff member's private life that are considered inappropriate to discuss with students.

4. Post or share information that identifies any student.

5. Disclose personally identifying information about coworkers or supervisors.

6. Post or share discriminatory or defamatory information.

7. Post or share comments that would cause a disruption in the educational environment.

8. Suggest through any personal social networking context that s/he in any way represents the school district or is speaking on behalf of the school district.

9. Violate any Board policy, including the district's policies on discrimination, harassment, privacy, and bullying.

District-Provided Mobile Devices

Mobile devices (including laptops, handhelds, cell phones, and tablet computers) may be provided to district employees for professional use both on and off the school grounds in order to enhance, enrich, and facilitate teaching and learning, to perform job-related tasks, and to enhance school communications. Mobile devices are to be used for professional duties, including but not limited to curriculum enhancement, research, district communications and other educational purposes. Users are expected to abide by this policy when using mobile devices both on and off the school network. Users are expected to treat these devices with great care and caution and must report any loss, damage, or malfunction to IT staff immediately. Failure to do so may result in the user being held financially accountable for any damage resulting from negligence or misuse. Additional guidelines relating to the acceptable use of mobile devices will be disseminated to faculty and staff members.

Hardware and Software

In order to maintain adherence to copyright law and to increase security and reliability of systems, users are expected to utilize hardware and software in a manner that enables its ongoing usage. To this end, district staff and students are responsible for informing the technical support staff immediately if, at any time, the hardware and/or software does not work properly. All district staff and students must respect all computer equipment peripherals. No attempt should be made to store any inappropriate materials on any district technology equipment. Users are, under no circumstances, to attempt to repair or reconfigure district-owned technology equipment in any way.

Printing

All the items in this policy apply to printers and the jobs that users send to the printers, including but not limited to, copyright, excessive use, personal use, inappropriate material and monitoring. Users can also refer to the guidelines in Policy 814 for specifics on copyright and photocopying.[9]

Home Use

The policy applies to both in school and at-home use for staff and students.

To ensure that students and staff use these educational resources responsibly while at home, it is imperative that the following provisions are understood:

1. No one other than the district employee or student uses his/her district-assigned account, laptop or equipment.

2. District policy for behavior and communication apply when using the Internet, according to the stipulations of this policy.

3. Users should have no expectation of privacy while utilizing their district-assigned account or computer at home.

4. In-home technology support should not be expected from district technology staff; it is the user's responsibility to report any problems with equipment immediately to the building Support Technologist.

5. Any and all costs incurred by the district for repairs caused by negligent use may be the financial responsibility of the user who caused the problem. Under no circumstances should the user attempt to take district-owned technology to a service provider nor should the user attempt to repair technology equipment himself/herself.

Additionally, families should be aware that some material accessible via the Internet might contain items that are illegal, defamatory, inaccurate, or potentially offensive to some people. Also, it is possible to purchase certain goods and services via the Internet, which could result in unwanted financial obligations for which a student's parent/guardian would be liable.

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 the guidelines put forth in the Digital Millennium Copyright Act (HR2281) and the Technology, Education and Copyright Harmonization (TEACH) Act. [9][10]

WEBSITE GUIDELINES

Unless otherwise approved, all district-sponsored and maintained websites (which includes all school, teacher or classroom web pages for educational purposes) must be hosted from district-owned and operated computer server(s) on school property and must adhere to procedures and guidelines outlined in this policy.

Rationale

School websites are public documents welcoming the outside world to the school and linking students and staff to outside sources of information. Guidelines are required in the construction of school web pages to ensure that information on the pages is appropriate for any Internet user to access and free from advertising or information items which may not be appropriate for students. The content of school websites must be consistent with the educational mission, goals, strategic plan and objectives of the district and Board policies. All district-sponsored and maintained websites are property of Bethlehem Area School District.

Disclaimer of Liability

The district IT Department does not warrant or guarantee access or data integrity of student or teacher-developed web content. Any and all web content created for class projects or course work should be backed up frequently using local resources.

The district IT Department reserves the right to immediately stop access to or from any site which may be in violation of this policy or otherwise poses a risk to the district's network, personnel or other technology resources.

CONSEQUENCES FOR INAPPROPRIATE USE

Violations of this policy may result in the loss of access, additional disciplinary action consistent with existing practice and policy, and/or appropriate referral to the authorities. The district will cooperate to the extent required with authorities in all investigations. Anyone witnessing a violation of this policy must report the violation to his/her immediate supervisor.[1][11]

Any user who violates provisions of this policy that cause damage to the network, computer equipment, electronic communications systems, or software will be held responsible for those damages. The user will also be responsible for incidental or unintended damage resulting from willful or deliberate violations of this policy.[6]

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