

Bremen Public Schools Technology Acceptable Use POLICY 346

1.0 Overview

Bremen Public Schools (herein “BPS”) provides technology to the classroom to support learning. The use of such technology shall be consistent with the curriculum adopted by BPS and/or activities required to support instruction or school operations. Effective security requires a team effort involving the participation and support of every BPS student and employee. Therefore it is the responsibility of every student and employee to know this policy and to conduct their activities accordingly.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of technology at BPS. Inappropriate use seriously impacts the learning process, exposes students and employees to objectionable matter, and/or may present legal issues.

2.1 Social Networking Education

The Corporation recognizes its responsibility to educate students regarding appropriate behavior on social networking and chat room sites about cyberbullying. Therefore, students shall be provided instruction about appropriate online behavior, including interacting with other individuals on social networking sites and in chat rooms and cyberbullying awareness and response.

3.0 Scope

This policy relates to all technology equipment owned by BPS or any other technology equipment utilized on BPS property.

4.0 Policy

Before using technology within Bremen Public Schools, all students and employees must read and understand this acceptable use policy. Additionally, by using any school technology a student or employee is agreeing to this policy whether or not it has been read and understood by the student or employee. Parents who do not agree with the rules regarding Internet usage should complete the Student Internet Non-Consent Form.

4.1 Privileges and Privacy

- When using BPS technology, students and employees shall have no expectation of privacy. Additionally, students and employees will consent to monitoring of their activity and if necessary seizing of the BPS technology assets and data without warning, prior consent or notice by school officials.
- Students and employees shall not hold BPS liable for any damage to assets or data due to harmful programs or viruses that may extend through the technology.
- BPS provides access to the Internet, but does not endorse all content found on the Internet.

4.2 General Use and Ownership Match

- Technology is made available to students and employees to support the educational process. This includes web-based assessment/testing programs, research materials, subject specific software, as well as any software or hardware which is used to support the curriculum and/or operations of the schools.
- For security and network maintenance purposes, authorized individuals within the BPS may monitor equipment, systems and network traffic at any time.
- BPS may audit networks and systems on a periodic basis to ensure compliance with this policy.

4.3 Security and Proprietary Information

- Students and employees may only access information and/or computer systems to which they are authorized.
- Students and employees must secure their electronic data and save it to a secure location such as the individual's home directory.
- Students and employees may not unlock computers from their security devices or remove computers from any BPS premises without the written permission from the Technology Director or Media Specialist.
- Students and employees may not remove inventory markings or tags from computers or other technical equipment.
- Students and employees may not disable or modify security settings or measures.
- Students and employees with network accounts are responsible for the security of their passwords and accounts.
- Students and employees should not open email attachments received from unknown senders as they may contain viruses that may harm BPS information.

4.4 Unacceptable Use

The following activities are prohibited. Under no circumstances is a student or employee of the BPS authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing BPS owned resources. The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the BPS.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which BPS or the end user does not have an active license in the BPS' name is strictly prohibited.
- Exporting software, technical information, encryption software or technology. The appropriate management should be consulted prior to export of any material that is in question.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others.
- Making fraudulent offers of products, items, or services originating from any BPS account.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee/student/user is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Executing any form of network monitoring which will intercept data not intended for the student, employee or other user's computing asset, unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host, network or account.

- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

Internet Activities

BPS uses Internet filtering software to protect its network and prevent students, employees or other users from viewing undesirable sites. This filtering software is required by federal law as a means to protect BPS' students. However, no filtering software is 100% effective, so students should access the Internet only with adult supervision. At no time is any BPS student or employee permitted to circumvent this software to access a denied site. Other prohibited activities include:

- Utilizing Internet "proxy" sites to circumvent Internet filtering software and filtered sites
- Accessing profane or obscene material, material suggesting illegal acts and/or material advocating violence or discrimination
- Posting personal contact information if you are a student
- Agreeing to meet someone online if you are a student
- Using obscene, profane, lewd, vulgar, inflammatory or threatening language
- Posting false or defamatory information
- Plagiarizing information found on the Internet

Email and Communications Activities

While not all students or employees have BPS-assigned email accounts, they might have personal email accounts (Gmail, Hotmail, Yahoo, etc.) that they can access through the BPS network and Internet connection. BPS cannot access, review, copy or delete any such messages sent, received or stored on the external email systems. Therefore students and employees are expected to adhere fully to the acceptable and unacceptable uses as outlined in this policy.

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment or cyberbullying via email, telephone, texting, or paging, whether through language, frequency, or size of messages.
- Any type of threats to persons, places, or things, including terrorist-related activities.
- Unauthorized use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

5.0 Enforcement

A violation of this policy by any student or employee may result in the cancellation of technology privileges, discipline, and/or criminal prosecution.

6.0 Legal References

- 47 U.S.C. 254(h)

