BRAINTREE PUBLIC SCHOOLS

Policy IJNDB

Network & Technology Responsible Use Policy

1. Introduction

This document formalizes the policy for responsible use of the Braintree Public Schools' (BPS) computer network and computing devices owned by BPS or used on the BPS campus. All users, including students, teachers, staff, administrators, and organizations are covered by this policy and are expected to be familiar with its provisions.

2. User Responsibilities

The BPS computer network and all related technology systems are designed and maintained in compliance with state and federal law, including the Children's Internet Protection Act and Protecting Children in the 21st Century Act Amendment. All use of the network to access the Internet is filtered via a firewall, and network activities harmful to minors or non-compliant with educational uses are prohibited (see Section 3). It is the responsibility of any person using BPS computer network resources to read, understand, and follow these guidelines. In addition, users are expected to exercise reasonable judgment in interpreting these guidelines and in making decisions about the appropriate use of BPS computer network resources. Any person with questions regarding the application or meaning of these guidelines should seek clarification from the BPS technology director or central office. Use of BPS computer network resources shall constitute acceptance of the terms of these guidelines. When a user is no longer a member of the BPS community, he or she shall no longer have user rights to network and technology resources.

A. BPS Computer Network Administrator Responsibilities

The administrator is responsible for making certain that all users understand and abide by the Acceptable and Unacceptable Uses as stated in this document (Section 3). If the BPS computer network administrator has reason to believe that any user is misusing the system, the administrator has the right to access the user's account in order to review its use. It is also the responsibility of the administrator to report any misuse of the system to district administrators.

B. BPS Computer Network Educator Responsibilities

It is the responsibility of educators who are using BPS computer network tools with students to teach students about safe and responsible use of the Internet and the network (see also BPS Internet Safety Policy). Educators are responsible for monitoring students' use of these resources and must intervene if students are using them inappropriately. Educators should make sure that students understand and abide by the Acceptable and Unacceptable Uses as stated in this document (Section 3). It is also the

responsibility of the teacher to report any misuse of the system to his/her building administrator.

C. BPS Computer Network Student Responsibilities

It is the responsibility of students who are using BPS computer network tools to learn about safe and responsible use of the Internet. They are responsible for using these resources appropriately. They must abide by the Acceptable and Unacceptable Uses as stated in this document (Section 3). If a student is misusing the system, educators must follow appropriate disciplinary protocols, including but not limited to reporting the misuse to the BPS computer network administrator, who has the right to discontinue his/her use of the system.

3. Acceptable and Unacceptable Uses

The resources available to BPS computer network users are to be used for educational purposes. Users should not use BPS computer network to store any files that are not educational. BPS will educate all students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response (see also BPS Internet Safety Policy).

It is unacceptable for users to use these resources for:

- furthering any political or religious purpose
- engaging in any commercial or fundraising purpose that is not relevant to or approved by the district
- sending threatening or harassing messages
- gaining unauthorized access to computer or telecommunications networks
- interfering with the operations of technology resources
- accessing or sharing sexually explicit, or obscene materials
- intercepting communications intended for other persons
- attempting to gain unauthorized access to the BPS computer network
- logging in through another person's account or attempting to access another user's password or files, except where necessary for a teacher or administrator to do so
- sending defamatory or libelous material concerning a person or group of people
- furthering any illegal act, including infringing on any intellectual property rights
- researching, storing, or sending information regarding weaponry, except in bona fide research as required by the district's curriculum (for example, an assignment studying a war)
- downloading, uploading, or distributing any files, software, or other material that is not specifically related to an educational project
- downloading, uploading, or distributing any files, software, or other material in violation of federal copyright laws

As with any other form of communication, these systems may not be used to transmit or store messages or other data that are prohibited under existing BPS policies, such as those

prohibiting sexual harassment, protecting civil rights, and maintaining a safe school environment. Users should take all reasonable precautions against receiving or downloading messages, images, or other data of this sort.

4. **Privacy Protections beyond BPS**

In compliance with state and federal privacy laws for minors accessing the Internet using school resources, BPS maintains a list of sites and services, along with the personally identifiable data on students that might be included as part of the terms of use for that site or service. Parents of children 13 and under retain the right to opt their students' out of participation in services that require use of personally identifiable data. BPS administration expects staff and students to adhere to the list of approved sites and services when selecting educational resources for use in the classroom (see also Section 8).

5. No Expectation of Privacy within BPS

BPS computer network resources are the property of the Braintree Public Schools and are to be used in conformance with these guidelines. BPS administration retains the right to inspect any user's virtual hard drive, school-owned computer, Internet history, or email (whether through a town server or through Google Apps for Education/G Suite) if a suspected violation of the network technology policy or any other district policy has occurred. In keeping with state and federal laws regarding public records, users should be aware that data and messages are regularly archived, even if they appear to have been deleted locally. In addition, an Internet firewall automatically checks all data moving between the local area network and the Internet and logs the sending and receiving destinations. Use of BPS Computer network technology resources constitutes consent for the BPS computer network staff to monitor and/or inspect any files that users create, any messages they post or receive, and any web sites they access should a disciplinary or safety situation warrant such access.

6. Passwords

Each user shall be required to use and maintain passwords that conform to BPS computer network guidelines. Users must take precautions to maintain the secrecy of their password so that other users will not be able to utilize that password for malicious purposes. If a user suspects that someone has discovered his or her password(s), the user should change the password(s) or contact technology services via the Help Desk for assistance in changing the password(s) immediately. BPS computer network users are responsible for all activity under their accounts.

7. Violations

Failure to observe these guidelines may subject users to termination of their BPS computer network accounts, including Google Apps for Education/G Suite accounts, email accounts, and accounts with other district-provided services. BPS administrators will be notified of any inappropriate activities by users, and users will be subject to recourse through other existing BPS policies as applicable. BPS administrators will also advise law enforcement agencies of illegal activities conducted through the BPS computer network and will cooperate fully with

local, state, and/or federal officials in any investigation related to illegal activities conducted through the BPS computer network.

7. Bring Your Own Device (BYOD) Uses

The use of personal electronic device(s) on a school site is a privilege, not a right, that the Braintree Public Schools grants to any student who is willing to assume the responsibility of abiding by the guidelines as set forth in this Braintree Public Schools' Technology Acceptable Use Policy. Noncompliance with applicable regulations may result in suspension or termination of privileges and other disciplinary action consistent with district policies.

Any student who receives approval from his or her classroom teacher to bring in an electronic device is also responsible for physically securing their device within the school site. Braintree Public Schools assumes no responsibility or financial liability for any damage the student or parent suffers, including but not limited to theft, physical damage, and loss of data or software malfunctions of the personal electronic device. If an electronic device appears to have been stolen, the student should immediately report the incident to the school administrator.

- Students (who have received permission) may connect wirelessly to the BPS network for educational purposes. Personal electronic devices may not be used for entertainment, including but not limited to games, messaging, social media, streaming movies, music, or video viewing, while connected to the BPS network, unless instructed to do so.

- Students must follow additional guidelines which a classroom teacher or BPS staff member might impose. The use of the electronic device(s) may in no way disturb the learning environment.

- Students are strictly prohibited from using peer-to-peer file sharing software and messaging programs unless instructed by a teacher to do so.

- Any student who is suspected of violating the Network & Technology Responsible Use Policy or any other BPS policy must yield their personal electronic device(s) to any Braintree Public Schools staff member upon request. Authorized personnel may inspect the system to determine whether any policies have been violated.

8. Disclaimers

The Braintree Public Schools make no warranties of any kind, either expressed or implied, for BPS computer–services and resources. BPS is not responsible for any damages incurred, including but not limited to the following: loss of data resulting from delays or interruption of service, loss of data stored on BPS computer network resources, or damage to personal property used to access BPS computer network resources. BPS is not responsible for the

accuracy, nature, or quality of information stored on BPS computer network resources or gathered through BPS computer network or the Internet. BPS is not responsible for unauthorized financial obligations incurred through BPS computer network-provided access. BPS accepts no liability for users who willfully ignore or violate terms of use on an Internet site or service via the BPS network. All provisions of this agreement are subordinate to local, state and federal statutes.

This policy is in compliance with state and federal telecommunications rules and regulations, including the Children's Internet Protection Act, the Protecting Children in the 21st Century Act Amendment, the Children's Online Privacy Protection Act, the Family Educational Rights and Privacy Act, and the Protection of Pupil Rights Amendment.

Acknowledgements: Sections of this document were adapted from Quincy Public Schools, Hanover Public Schools, and Burlington Public Schools, the Massachusetts Office of Digital Learning, FCC and FTC recommendations, and federal laws.

Adopted by the Braintree School Committee, 6/12/2017