Brentwood Borough School District Acceptable Use Policy 815

Purpose

The Brentwood Borough School District provides its employees, students, and guests ("users") access to technology resources including, but not limited to, electronic communications systems, computers, computer networks, networked devices, hardware, software, internet access, mobile devices, peripherals, copiers, and cameras.

The Board supports use of the district's technology resources to facilitate learning and teaching, to provide access to information, to aid in research and collaboration, to foster the educational mission of the district, and to carry out the legitimate business and operation of the district.

The use of the district's technology resources is for appropriate school-related educational and operational purposes and for the performance of job duties consistent with the educational mission of the district. **Use for educational purposes** is defined as use that is consistent with the curriculum adopted by the district as well as the varied instructional needs, learning styles, abilities and developmental levels of students. All use for any purpose must comply with this policy and all other applicable codes of conduct, policies, procedures and rules and must not cause damage to the district's technology resources.

All employees and students are responsible for the appropriate and lawful use of the district's technology resources. This policy is intended to ensure that all users continue to enjoy access to the district's technology resources and that such resources are utilized in an appropriate manner and for legitimate purposes.

Authority

The Board establishes that access to and use of its technology resources is a privilege, not a right, which may be revoked at any time. The district's technology resources are the property of the district. The district provides these resources for educational and operational purposes as stated herein and are not provided as a public access service or to provide a public forum.

The Superintendent and his/her designee is ultimately responsible for overseeing the district's technology resources. The Superintendent will designate a network administrator who will serve as the coordinator and supervisor of the district's technology resources and networks, and who will work with other regional and state organizations as necessary to

educate users, approve activities, provide leadership for proper training for all users in the use of the district's technology resources and the requirements of this policy, and who will establish a system to ensure that users who access district technology resources have agreed to abide by the terms of this policy.

The Superintendent or his/her designee is directed to implement internet safety measures to effectively address the following, both through general policy and through the use of filtering technology:

1. Access by minors to inappropriate or harmful content.

2. Safety and security of minors when using electronic mail, chat rooms, and social networking.

3. Prevention of unauthorized access of district technology resources.

4. Prevention of unauthorized disclosure and dissemination of minors' personal information.

Definitions

District Technology Resources: District technology resources means all technology owned, operated, and/or licensed by the district, including computers, projectors, televisions, video and sound systems, mobile devices, calculators, scanners, printers, cameras, portable hard drives, hardware, software, accounts, routers and networks, including the internet.

User: User means anyone who utilizes or attempts to utilize district technology resources while on or off district property. The term includes, but is not limited to, students, staff, parents and/or guardians, and any visitors to the district that may use district technology.

Guidelines

Unauthorized Use Prohibited

Only users who have agreed to abide by the terms of this policy may utilize the district's technology resources. Unauthorized use, utilizing another user's district account, or exceeding one's authorization to use district technology resources is prohibited. Nothing in this policy, however, shall prevent a parent and/or guardian from assisting his/her child with the use of the district's technology resources, or from monitoring a student's use of the district's technology resources in the student's home.

Use of Personal Electronic Devices

The use of personal electronic devices on the district network is permitted only on designated networks. When a user connects a personal electronic device to a district network or district technology resources, this policy and its guidelines apply. Users are subject to the same levels of monitoring and access as if a district-owned device were being utilized. Users who connect a personal electronic device to a district network explicitly waive any expectation of privacy in the content exchanged over the district technology resources.

Privacy

The district reserves the right to monitor any user's utilization of district technology resources. Users have no expectation of privacy while using district technology resources whether on or off district property. The district may monitor, inspect, copy and review any and all usage of district technology resources including information transmitted and received via the internet, to ensure compliance with this and other district policies and state and federal law. All emails and messages, as well as any files stored on district technology resources, may be inspected at any time for any reason. The district may decrypt and inspect encrypted internet traffic and communications to ensure compliance with this policy.

Internet Filtering and CIPA Compliance

The district utilizes content and message filters to prevent users from accessing material through district technology resources that has been determined to be obscene, offensive, pornographic, harmful to minors, or otherwise inconsistent with the district's educational mission. The Superintendent or his/her designee shall establish a procedure for users to request that a legitimate website or educational resource not be blocked by the district's filters for a bona fide educational purpose. Such requests must be either granted or rejected within three (3) school days pursuant to the established procedure.

The Board directs that the Superintendent or his/her designee ensure that students at the elementary, middle school, and high school levels are educated about appropriate online behavior including interacting via social networks and in chat rooms, cyberbullying, and disclosure of personal information.

Monitoring

District technology resources shall be periodically monitored to ensure compliance with this and other district policies including monitoring of

users' online activities. The network administrator designated by the Superintendent shall ensure that regular monitoring is completed pursuant to this section. However, the Superintendent or his/her designee shall also implement procedures to ensure that district technology resources are not utilized to track the whereabouts or movements of individuals, and that remotely activated cameras and/or audio are not utilized except where necessary to recover lost or stolen district technology.

District Provided Resources

District technology resources may be assigned or allocated to an individual user for his or her use (e.g., individual email accounts, laptop computers, etc.). Despite being allocated to a particular user, the technology resources remain the property of the district and may be revoked, suspended, or inspected at any time to ensure compliance with this and other district policies. Users do not have an expectation of privacy in any district provided technology resource or any of its contents.

Students are expected to act in a responsible, ethical, and legal manner in accordance with the district policy, accepted rules of network etiquette, and federal and state law. Specifically, the following uses are prohibited:

The following uses of district technology resources are prohibited:

1. Use of technology resources to violate the law, facilitate illegal activity, or to encourage others to do so.
2. Use of technology resources to violate any other district policy.
3. Use of technology resources to engage in any intentional act which might threaten the health, safety, or welfare of any person or persons.
4. Use of technology resources to cause or threaten to cause harm to others or damage to their property.
5. Use of technology resources to bully, or to communicate terroristic threats, discriminatory remarks, or hate.
6. Use of technology resources to communicate words, photos, videos, or other depictions that are obscene, indecent, vulgar, rude, profane, or that advocate illegal drug use.
7. Use of technology resources to create, access, or to distribute obscene, profane, lewd, vulgar, pornographic, harassing, or terroristic materials, firearms, or drug paraphernalia.
8. Use of technology resources to attempt to interfere with or disrupt district technology systems, networks, services, or equipment including, but not limited to, the propagation of computer "viruses" and "worms," Trojan Horse and trapdoor program codes.

9. Altering or attempting to alter other users' or system files, system security software, system or component settings, or the systems themselves, without authorization.
10. The attempted physical harm or attempted destruction of district technology resources.
11. Use of technology resources in a manner that jeopardizes the security of the district's technology resources, or in a manner that attempts to circumvent any system security measures.
12. Use of technology resources to intentionally obtain or modify files, passwords, and/or data belonging to other users or to the district.
13. Use of technology resources that conceals or attempts to conceal a user's identity, including the use of anonymizers or the impersonation of another user.
14. Unauthorized access, interference, possession, or distribution of confidential or private information.
15. Using technology resources to send any district information to another party, except in the ordinary course of business as necessary or appropriate for the advancement of the district's business or educational interests.
16. Use of technology resources to commit plagiarism.
17. Installing, loading, or running software programs, applications, or utilities not explicitly authorized by the district technology staff.
18. Installing unauthorized computer hardware, peripheral devices, network hardware, or system hardware onto technology resources.
19. Copying district software without express authorization from a member of the district's technology staff.
20. Use of technology resources for commercial purposes.
21. Use of technology resources for political lobbying or campaigning, not including student elections (e.g., student government, club officers, homecoming queen, etc.)
22. Use of district technology resources to tether or otherwise connect to a non-district owned device to access an unfiltered and/or unmonitored internet connection.
23. The use of proxies or other means to bypass internet content filters and monitoring.
24. The use of technology resources to gamble.
25. Unauthorized access into a restricted system or changing settings or access rights to a restricted system or account.
26. The use of encryption software that has not been previously approved by the district.
27. Sending unsolicited mass email messages, also known as spam.
28. Scanning the district's technology resources for security vulnerabilities.

Consequences for Inappropriate Use of District Technology

Violations of this policy may result in the temporary or permanent revocation of a user's right to access district technology resources. Additionally, students may be subject to other forms of disciplinary actions for violations of this policy and/or local, state, and/or federal law.

Limitation of Liability

The district makes no warranties of any kind, whether express or implied, for the service it is providing through its various technology resources. The district is not responsible, and will not be responsible, for any damages, including loss of data resulting from delays, non-deliveries, missed deliveries, or services interruption. Use of any information obtained through the district's technology resources is at the user's own risk.

BBSD ACCEPTABLE USE AGREEMENT AND PARENT PERMISSIONS

Please fill out this form out electronically or use blue or black ink. Have your child turn in the completed form to the main office or bring it with you to device distribution. Elementary students can print their name on the signature line.

LAST NAME of student (please print) | *FIRST NAME of student (please print)*

Student ID # | *Grade Level*

LAST NAME of parent (please print) | *FIRST NAME of parent (please print)*

Home Address | *City, State, Zip*

Home Phone | *Email Address*

Student:

Network: As a user of the Brentwood School District computer network, I hereby agree to comply with the statements and expectations outlined in the Brentwood Borough School District Student Network/Internet User Agreement and to honor all relevant laws and restrictions. I also agree to use the network responsibly.

Device: Having fully read the Brentwood Borough School District device agreement, I understand my responsibilities for caring for the computer, and I agree to the terms regarding the device I will receive from the Brentwood Borough School District.

STUDENT SIGNATURE *DATE*

Parent:

Network: All students are provided with access to district computer resources. In addition to accessing our district computer network, as the parent or legal guardian, I grant permission for my student to access the Internet. These permissions are granted for an indefinite period of time unless otherwise requested. I understand that individuals and families may be held liable for violations. I understand that some materials on the Internet may be objectionable, but I accept responsibility for guidance of Internet use and will set standards for my child(ren) to follow when selecting, sharing, or exploring information and media.

Device: Having fully read the Brentwood Borough School District device agreement, I understand my responsibilities for caring for the computer, and I agree to the terms regarding the device my child will receive from the Brentwood Borough School District.

Device Return: I understand that the device and charger must be returned to my child's school on the last day of school each academic year or on a date pre-determined by school administrators. Failure to turn in the device and charger may result in the collection being turned over to the magistrate and my child will be prohibited from participating in any extra-curricular activities including, but not limited to, athletics, clubs, after school events, graduation, and/or anything beyond the regular school day or curriculum. I also understand that a new device will not be issued to my child until any outstanding device obligations have been satisfied.

PARENT/GUARDIAN SIGNATURE *DATE*

2020-21 BBSD TECHNOLOGY PROTECTION PLAN

This is an optional and voluntary program available to all students/parents

Please read this entire document to determine if this program is needed for you and your child's protection against damage of the BBSD device in your care. This form must be completed and marked YES (with payment attached) or NO before the device will be provided to the student.

Coverage and Benefit

This agreement covers the BBSD device loaned to the student against some incidents of accidental damage. The following items are **NOT** covered:

- A device that is lost or stolen
- Damage caused by negligence including but not limited to leaving it outside in an automobile, immersion in liquid, any type of damage caused by food or drink, damage caused by pets, rough/inappropriate handling, etc.
- Intentional misuse of one's own or a peer's device
- More than one accidental incident, including more than one broken screen or accessories.
- Loss of power adapter/cord

Effective and Expiration

This coverage is effective from the date this Plan form and premium payment are received by the school through the date when the device is to be returned in good working condition to the school or at least by the end of the current school year.

Premium

The current total premium cost is $20 paid annually. The premium for students that qualify for free and reduced lunch is $10 paid annually. Partial semesters/years are not refundable.

There is a discount for multiple students living in one household:

- Two students - $30.00 paid annually
- Three or more students - $40.00 paid annually

It is agreed and understood that:

- A separate signed application will be needed for each device covered.
- It will be the right of the principal or his/her designee to determine if damages were due to negligence or accidental in nature.
- The principal reserves the right to determine cost of repair/replacement and to assess such charges. Students must clear all device fees before participating in school-related events, including attendance at sports, dances, and graduation.
- The principal will review all damages determined to be from misuse or negligence and will assess the student's continued privilege of taking the device to and from school.

Please complete the information below and bring this completed form to Chromebook Distribution or to the Computer Para(s) during the school year:

_____

LAST NAME of student (please print) *FIRST NAME (please print)*

_____

Student ID # *Grade Level*

_____

Home Address

_____

City, State, Zip

_____

Home Phone

☐ **YES**, I would like to participate in the Technology Protection Plan. My payment is attached. Make checks **payable to "Brentwood Borough School District"**

☐ **NO**, I decline the Technology Protection Plan service at this time. I understand I am responsible for 100% of any damage or loss to the BBSD device. The current replacement cost of a device power adapter, and cord is between $200-$300 depending on the age and model of the device.

_____

Parent/Guardian Signature *Date*

FOR INTERNAL USE ONLY

Date_____Recorded by _____

Check #_____Cash_____MO _____