BBSD Student Device Guide

BBSD Technology Staff:

Technology Director: Melissa Fulmer

IT Technician: Joe Scuilli

Support Email: mailto:servicedesk@bb-sd.com

Support Voicemail: 412-437-3621

Please provide your name, your student's name, a good phone number/email to reachyou, and a detailed description of your issue.

About the Chromebook/Surface Laptop

This guide contains information on using the school-issued Chromebook (Grades K-5) and Surface Laptop (Grades 6-12), expectations for learning, care and handling of the device, and basic troubleshooting tips.

BBSD provides a Chromebook (Acer or Dell) or Microsoft Surface Laptop SE enclosed in a protective case and a charger to each student to be used as an educational tool.

As the Chromebooks/Surface Laptops are property of the Brentwood Borough School District, all activity including, but not limited to, device usage and email can and will be monitored.

General Chromebook/Surface Laptops Use and Care

Each device has unique identification numbers and is assigned to a specific student. The names and numbers on the device and case are registered to the Brentwood Borough School District. Students are not to switch devices with other students. **STUDENTS MAY NOT REMOVE ANY ID FROM THE DEVICE.**

Devices should never be left unattended or unsecure in areas (e.g., unlocked locker or classroom), and should never be stored in vehicles.

Handling

Use a soft, clean cloth to clean the screen, and never use any sort of cleanser. The keyboard may be disinfected by using a wipe. Be sure that the device is powered off and the wipe is not excessively wet. **Important:** Do not use the wipe on the screen. Allow the device to dry before powering back on. Do not expose the device to extreme heat or cold and keep it away from food and drinks.

Cords and Cable Care

- Cords and cables require delicate care when inserting or removing them from the device. Examples of cords and cables include the charger, Ethernet cable, and/or wireless USB mouse.
- The charging cable must be treating gently, and should not be tightly wound, crimped, or pulled on. Rough handling of the cord will damage it to the point where it will no longer charge the device. Ideally, the charger should stay in a single location where the device can be plugged in for overnight charging.

Personalizing Devices or Cases

- **Do not** mark or "personalize" the device. You *may* personalize the **case**. We recommend using stickers to do so. This will help distinguish your Chromebook from others.
- Device screens are made of glass and are particularly sensitive to damage from impact and pressure. If the screen chips or cracks, **do not attempt to fix it.** Bring it to the attention of the school principals, building administrators, or IT department via the contact information on the front page of this packet.
- Every device has a protective case. The device must be kept within the case at all times. If damage occurs as a result of the device being out of the case, all costs related to the damage will be incurred by the student.

Important: If the device or charger becomes damaged, please refer to the device insurance document for fees and notify the school principal, building administrator, and/or the IT department.

Expectations for Student Learning

- The device is an educational tool, not an entertainment device, and should be used as such.
- Be sure to keep the device charged and ready to go for the day.
- Keep the operating system (Chrome OS) and apps up to date.
- Use the device to complete class work or independent work assigned by your teachers, and refrain from using it in any ways that violate the terms of the Acceptable Use Policy (AUP), including playing games and watching movies.

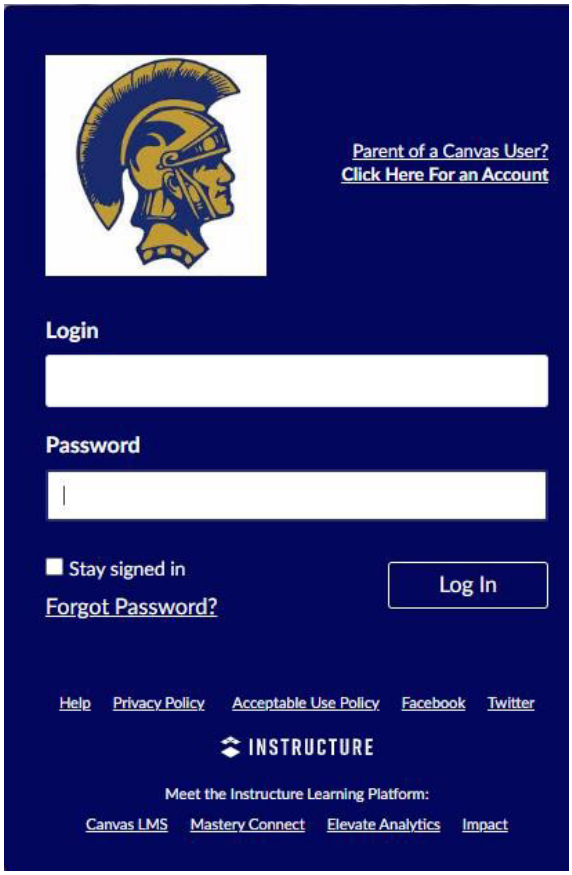
If any of the above requirements become an issue, the student will be referred to administration and the technology director.

Signing into your Device

- In order to sign into the device, use your school email: firstname.lastname@bb-sd.com. Your password is "bbsd" followed by your school lunch code. *Example: bbsd123456.* If you get locked out of your account, contact support to have your password reset and your account unlocked.

Canvas Learning Management System

During the 2020-2021 school year, the district adopted the Canvas Learning Management system. Canvas allows our teachers to build upon their work to utilize these resources in a true learning management system that will meet the needs of students, teachers, and families. Please reference the district's website and information shared by your student's teachers for more detailed information about Cnavas.



- To log into Canvas, go to bbsd.instructure.com and enter your school email. Your password is your school lunch code *only* (no "bbsd" at the beginning.)
- To log into Kami, on the Kami login screen, click "With Google," and use the same login information that you used to sign into the Chromebook.

Canvas Guide

It is recommended that you set up an observer account to access your child's courses and grades. There is a video available on the district's website, www.bb-sd.com, under the "Parent" tab, with instructions on creating an account.

Canvas Guide for Parents and Students

STEP 1: LOG IN TO THE ACCOUNT

- Go to www.bb-sd.com
- Click on the Canvas icon.
- Enter username (first name.last name@bb-sd.com)
- Enter password (student ID number)

STEP 2: Access the class

- Once your login you should see your dashboard.

Send a message to the teacher:

- On the left hand side, you will see a button called "inbox". Click this. You will then see a button in the top right hand corner, it will be a leaf and say compose a message. Find your course and the correct teacher to send it to. Type your message, then hit send.

Using the Dashboard:

- The dashboard is a place where you will see all of the courses your child is enrolled in. Simply click on your homeroom course and begin working!

To complete an Assignment:

- Follow the directions that your teacher has provided. Once you are finished click Submit Assignment and it will guide you through how to submit the assignment.

Using the Calendar:

- To access the calendar, look on your left hand side then click the calendar button.
- The calendar will show you your assignments for each course (this will be color coded).

How to use Conferences:

To open a conference, go to the left hand side of your screen and click "Conferences". This will show you details about new and previous conferences that have or will be held.

- To join a session in progress, click the blue button on the right side that says 'Join'.
- To view an old conference, a link will be posted on the bottom of the conference box.

How to Use a Discussion Board:

To open a discussion board, look on the left hand side of your screen and click on the button "Discussions". This will take you to the discussions page.

- Discussions: these are current discussions within the class. You will only see the heading.
- Pinned Discussions: These are discussions that the teacher wants you to pay close attention to. THEY ARE IMPORTANT!!!
- Closed for Comments: This means this discussion has passed the due date and is turned off by the teacher.

Basic Troubleshooting

Some common problems and solutions are discussed below. E-mail support is also available by sending an email to servicesek@bb-sd.com or calling 412-437-3621 to leave a BRIEF message. You WILL receive a return phone call or email within 48 business hours.

- If a page is not loading, make sure you are still connected to the internet and click or tap the refresh button  .
- If you are getting an “access denied” error either within Canvas or Kami, contact your teacher *first* before contacting support. This might be as easy as a misconfigured document share.
- Try the “turn it off then back on” trick. Power the device completely off, wait 15-30 seconds, then power it back on to see if that fixes your problem.
- Try clearing the cache and cookies:
  - Click on the Chrome menu  on the top right of the Chrome browser.
  - Select “More Tools.”
  - Select “Clear Browsing Data.”
  - In the dialog that appears, select “Advanced,” then click on the “Time Range” box and select “All Time,” then check all the checkboxes.
  - Click “Clear Data.”
- If the keyboard settings were changed, hit SHIFT-ALT to set it back to US keyboard.
- If the image on the home screen is rotated: CTRL-SHIFT-REFRESH will rotate the entire screen by 90 degrees each time it is pressed.
- No sound? Try hitting the mute button.
- If you are running out of space on the Chromebook, delete unused files within your Downloads, located in your Google Drive.
- If the Chromebook won’t charge after plugging it in, try unplugging it, waiting 15-30 seconds, and plugging it back in.
- Are your Kami submissions not making it back to Canvas? Be sure you are signed into the correct Google Account and try again.
  - If Kami is not working correctly, you can see if Kami is down at status.kamihq.com. In most cases, if this page says there is a problem, ***there is nothing on our end that we can do to fix it.*** We monitor this page daily, so we are aware of any issues as well.

Lost, Missing, or Stolen Device

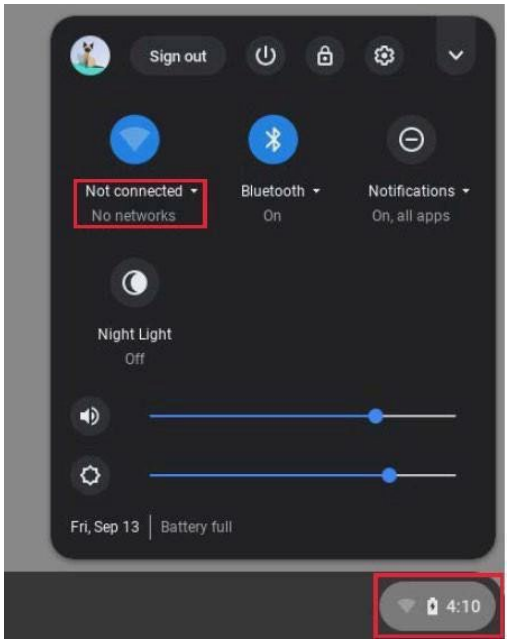
From the time the device is issued until the time the device is returned to the school, the student/family is responsible for it. If the device is not recovered, the student will be charged for replacement. If the student/family has purchased insurance, the expense *may* be covered.

If the device is **lost, missing, or stolen**, the student must report it to the school district immediately. The student should also contact servicedesk@bb-sd.com.

If a device is **stolen**, the student/family must report it to the school AND file a police report. A copy of the police report must be provided to the school.

Connecting to the Internet

To connect the device to your home Internet, click on the time on the bottom corner of the screen, then click on the network or Wi-Fi symbol. Click on your home network and enter your password to connect.



Home Internet

The Brentwood Borough School District realizes that not every family has access to the Internet at home. For those who wish to pursue Internet services, below is a curated collection of resources for families to obtain broadband Internet at their home at low or no cost.

- **Hotspot**: Many smart phones can be turned into a “hotspot” for use by other devices. Depending on your provider and plan, this may be either free or a small additional charge to your service. Contact your provider for details.
- **Comcast Internet Essentials**: Visit www.internetessentials.com for more details.
- **USAC** (a funding branch of the FCC): Discounts provided to qualifying families on their home Internet service through a program called Lifeline. Visit www.fcc.gov/consumers/guides/lifeline-support-affordable-communications for more details.
- **Verizon Lifeline Plans**: If you are approved for the Lifeline discount through USAC, you can apply it to your Verizon account. Visit www.verizon.com/support/residential/account/manage-account/lifeline-discount for more details.

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.

Procedures for Damages Not Covered

1. Did not purchase annual Device Protection Plan
    a. The Technology Department will assess damage and determine the cost to fix the device.
    b. The Technology Department will assess damage and determine cost to fix the device.
    c. The Technology Department will provide a written explanation via email of why the damage was not covered by the Device Protection Plan.
    d. A record of the invoice and any payments received will be recorded at the building level and will be listed as an obligation of the student, until the cost of the repair is paid in full.
2. Device Protection Plan purchased but repair not covered; device determined to be lost, stolen, vandalized, neglected, or has multiple accident claims.
    a. The Technology Department will assess damage and determine the cost to fix the device.
    b. The Technology Department will assess damage and determine cost to fix the device.
    c. The Technology Department will provide a written explanation via email of why the damage was not covered by the Device Protection Plan.
    d. A record of the invoice and any payments received will be recorded at the building level and will be listed as an obligation of the student, until the cost of the repair is paid in full.

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 andmedia.

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*

Please complete the information below and bring this completed form to Chromebook Distribution or to the building secretary during the school year: