13815 Spelling Court
Reno, NV 89521
775-851-5600
Fax 775-851-5605

Angie Bryan, Principal
email:
abryan@washoeschools.net

Brown Parent/Student Device Use and Agreement Handbook

Disclaimer: This document may contain references to Board Policies and other documents pertaining to the rules and regulations of the Washoe County School District. The District reserves the right to revise any of these documents during the course of the school year. For the current version of any of these documents, please check the District's website at www.washoeschools.net/Policy.

Non-Discrimination Statement: The Washoe County School District is committed to nondiscrimination on the basis of race, color, national origin or ethnic group identification, marital status, ancestry, sex, sexual orientation, gender identity or expression, genetic information, religion, age, mental or physical disability, military or veteran's status in educational programs or activities, and employment as required by applicable federal and state laws and regulations. No District employee, including, without limitation, administrators, faculty, or other staff members, nor students shall engage in acts of bullying, harassment, or discrimination on the premises of any public school, school-sponsored event, or school bus in the District. Prohibited behaviors include cyber-bullying, sexual harassment, hazing, intimidation and retaliation.

Overview

The District views the use of electronic resources as central to the delivery of its educational program and expects that all students will use electronic resources as an essential part of their learning experience. It is the policy of the District to maintain an environment that promotes ethical and responsible conduct in all electronic resource activities. With this privilege, come responsibilities for the parent/guardian and for the student.

Signing this Agreement

When signing the Student/Parent Device Agreement, you are acknowledging that you understand and accept the information in this document.

1. All users of the District's network and equipment must comply at all times with WCSD Administrative Regulation 7211 Responsible Use and Internet Safety Policy
2. Devices are on loan to students and remain the property of the District. District devices should be used solely for students' educational purposes and shall not be used for personal use unrelated to school assignments and lessons.

3. All users are accountable to District policies, regulations, and procedures, and local, state, and federal laws and regulations.
4. Use of the device and network must support education
5. Students and families must follow all guidelines set forth by the District and in this document.
6. All rules and guidelines are in effect before, during, and after school hours, for all District computers whether on or off the school campus.
7. All files stored on District equipment, the network, or cloud services are property of the District and may be subject to review and monitoring
8. The term "equipment" refers to devices, batteries, power cord/chargers, and peripherals (stylus, mouse, etc.) and cases. Each piece of equipment is issued as an educational resource. The term "device" includes laptops, tablets, notebooks, and desktop computers.
9. Students are expected to keep the devices in good condition. Failure to do so may result in fees for repair or replacement.
10. Students are expected to report any damage to their computer by the next school day.
11. Students who identify or know about a security problem are expected to convey the details to a staff member without discussing it with other students.
12. Students are expected to notify a staff member immediately if they come across information, images, or messages that are inappropriate, dangerous, threatening, or make them feel uncomfortable.
13. All users are expected to follow existing copyright laws and educational fair use policies.
14. Students should only log in under their assigned username. Students should keep their username and passwords private.
15. Students may not loan device components to other students for any reason. Students who do so are responsible for any loss of components.
16. Devices come with a standardized image already loaded which should not be modified in anyway.
17. All students have access to a network drive on which to store data (OneDrive). It is the responsibility of the student to see to it that critical files are saved regularly to this location.
18. The District may remove a user's access to the network without notice at any time if the user is engaged in any unauthorized activity.
19. The student understands that the assigned device and any equipment associated with it is subject to inspection at any time without notice and remains the property of the District.
20. The District reserves the right to confiscate the equipment at any time if there is reasonable suspicion that the student is violating a civil or criminal law or if the student is otherwise violating District policy, regulation, or procedure.
21. The use of the District's technological resources is a privilege, not a right, and is not transferable or extendible by students to people or groups outside the District.
22. The use of the assigned device and its associated equipment terminates when a student is no longer enrolled in Brown ES.
23. All assigned equipment must be returned to Brown ES at the time of withdrawal from the school.

Parent /Guardian Responsibilities

Overview – Parent/Guardian Responsibilities

The District makes every effort to equip parents/guardians with the necessary tools and information to ensure safe use of the devices in the home. The District has adopted a K- 12 digital citizenship curriculum through Common Sense Media to train students in using technology tools appropriately, which is a life skill. In order for students to be allowed to take their devices home, a student and their parent/guardian must have viewed all WCSD videos pertaining to device use and sign the Student/Parent Device and Use Agreement. The WCSD videos will cover the following topics:

- WCSD Electronic Use Policy and Acceptable Use Procedure
- Internet safety

- Parent/guardian and student responsibilities
- Brown ES policies and procedures.

Liability

The parent/guardian and student are personally responsible for the cost of repair or replacement if the equipment is:

- Not returned
- Intentionally damaged
- Lost because of negligence
- Stolen

Monitoring Student Use

The parent/guardian must agree to monitor student use of the device outside of the school day. The best way to keep students safe and on-task is to have a parent/guardian present and involved. The parent/guardian may choose to:

- Investigate and apply parental controls available through your internet service provider and/or your wireless router.
- Develop a set of rules/expectations for device use at home. Some websites provide parent/child agreements for you to sign.
- Only allow device use in common rooms of the home (e.g., living room or kitchen) and not in bedrooms.
- Demonstrate a genuine interest in what your student is doing on the device. Ask questions and request that they show you their work often.

Device Rules and Guidelines

Overview – WCSD Acceptable Use and Internet Safety Policy

The rules and regulations are provided here so that students and parents/guardians are aware of the responsibilities students accept when they use a District-owned device. In general, this requires efficient, ethical and legal utilization of all technology resources. ***Violations of these rules and guidelines may result in disciplinary action.***

General Guidelines

- All use of technology must:
  - Support learning
  - Follow local, state, and federal laws
  - Be school appropriate

Security Reminders

- Do not share logins or passwords with anyone.
  - Parents/guardians will receive separate access codes.
- Do not develop programs to harass others, hack, bring in viruses, or change others' files.

Follow internet safety guidelines (WCSD Administrative Regulation 7211)

Appropriate Content

All files must be school appropriate. Inappropriate materials include explicit or implicit references to:

Alcohol, tobacco or drugs

- Gangs
- Obscene language or nudity
- Bullying or harassment
- Discriminatory or prejudicial behavior

Prohibited Actions

- Students are prohibited from:
  - Defacing the device in any way. This includes but is not limited to marking, painting, drawing or marring any surface of the device.
  - If such action occurs, the student will be charged the cost of repair or replacement.
  - Putting stickers or additional markings on the device, battery, or power cord/charger.
  - If such action occurs, the student will be charged the cost of repair or replacement.
  - Leaning on the top of the device when it is closed.
  - Placing anything on top of the device that can put pressure on the screen.

Email for Students

All District students are issued a Microsoft Office 365 email account. This account allows students to safely and effectively communicate and collaborate with District staff and classmates, giving them an authentic purpose for writing. It is important to note:

- Email should be used for educational purposes only.
- All email and all contents are property of the District and can be accessed by the District.
- Email should only be used by the authorized owner of the account.
- Students need to protect their passwords.
- Students are limited to sending and receiving email only within the District.
- Mailbox size is restricted.
- Emails should not contain profanity, obscenity, derogatory, offensive or discriminatory language.
- Email should not be used for:
  - Non-education related forwards (e.g. jokes, chain letters, and images)
  - Harassment
  - Cyber-bullying, hate mail, discriminatory remarks
  - Individual profit or gain, advertisement, or political activities

Examples of Unacceptable Use

- Using the network for illegal activities, including copyright, license or contract violations.
- Unauthorized downloading or installation of any software including shareware and freeware.
- Using the network for financial or commercial gain, advertising, or political lobbying.
- Accessing or exploring online locations or materials that do not support the curriculum and/or are inappropriate for school assignments.
- Vandalizing and/or tampering with equipment, programs, files, software, network performance or other components of the network; use or possession of hacking software is strictly prohibited.
- Gaining unauthorized access anywhere on the network.
- Revealing the home address or phone number of one's self or another person or any other act that may invade the privacy of other individuals.
- Using another user's account or password or allowing another user to access your account or password.
- Coaching, helping, observing, or joining any unauthorized activity on the network.

- Posting anonymous messages or unlawful information on the network.
- Participating in cyber-bullying or using objectionable language in public or private messages, e.g., racist, terroristic, abusive, sexually explicit, threatening, stalking, demeaning or slanderous.
- Falsifying permission, authorization, or identification documents.
- Obtaining copies of, or modifying files, data, or passwords belonging to other users on the network.
- Knowingly placing a computer virus on a computer or network.
- Attempting to access or accessing sites blocked by the WCSD filtering system.
- Downloading music, games, images, videos, or other media without the permission of a teacher.
- Using the webcam inappropriately.
- Sending or forwarding social or non-school related email.
- Accessing or deleting the administrative account.

Device Security

Balanced Approach

Two primary forms of security exist: device security and internet filtering. Each device has a security program installed. The District strives to strike a balance between usability of the equipment and appropriate security to prevent damage to the District network.

Device Security

Security is in place on the device to prevent certain activities. These include downloading or installing software or browser extensions on the devices, removing software, changing system settings, etc.

Internet Filtering

The District abides by the Children's Internet Protection Act (CIPA): https://www.fcc.gov/consumers/guides/childrens-internet-protection-act and maintains an on-site internet filtering software package. This program automatically filters all student access to the internet through the District device, regardless of where the student is using the device.

Damaged/lost/stolen Equipment

Repairs

Occasionally, unexpected problems do occur with the devices that are not the fault of the user (computer crashes, software errors, etc.). The school tech support team will assist students with having these fixed. These issues will be remedied at no cost.

Lost or Stolen Equipment

Lost Equipment

•If any equipment is lost, the student/parent/guardian must report it to the school immediately (within one school day).

•The circumstances of each situation involving lost equipment will be investigated individually. Students/parent/guardian may be charged for lost equipment.

Stolen Equipment

- If equipment is stolen, the student/parent/guardian must report it to the school immediately (within one school day).
- Upon investigation, if there is no clear evidence of theft, or the equipment has been lost due to student negligence, the student/parent/guardian will be responsible for the full cost of replacing the item(s).
- Failure to report the theft may result in a fee for full replacement cost to the student.

Financial Responsibility

There is a cost ($10.00) for the receipt of a student laptop from the Washoe County School District. By accepting the District-owned laptop, parents/guardians are accepting full responsibility for the repair or replacement cost of the device. Each device will be assigned to one particular student for the duration of the school year and therefore it is the responsibility of the student to maintain control and possession of the device at all times in compliance with District directives.

ANY damaged, lost or stolen devices must be reported immediately to District personnel.