# 8320 Weber School District Student Appropriate Use Policy

I. PURPOSE AND PHILOSOPHY

The Weber School District Board of Education believes that the use of technology for information acquisition, retrieval, manipulation, distribution, and storage is an important part of preparing children for the 21st century. A "technology-rich" classroom can significantly enhance both the teaching and learning process. The district's technology resources, including computer hardware, software, local and wide-area networks, and Internet access, are provided for educational purposes that promote and are consistent with the instructional goals of the Weber School District. This policy outlines rules and guidelines for acceptable use to serve the educational needs of students.

II. POLICY

District-owned technology resources, including devices, networks, and Internet access, are provided to support educational purposes that align with the district's instructional goals. Use of these resources carries with it the responsibility to act in a safe, respectful, and lawful manner. All students are expected to follow the rules of appropriate use, which include protecting personal information, respecting others, and avoiding inappropriate, illegal, or disruptive activities. The district reserves the right to monitor and review all use of technology resources to ensure compliance with this policy and applicable law.

III. DEFINITIONS

A. **District-owned device(s)**: A device used for audio, video, text communication, or other computer-like instrument, identified as being owned, provided, issued, or lent by the district or individual school to a student or employee. A "school computer" as used in this policy is considered a district-owned device.

B. **Inappropriate material:** Any content—whether text, images, audio, video, or other digital media—that is not suitable for the school or district educational environment.

C. **District network resources**: District-owned technology that is not a district-owned device issued to students, including, but not limited to, servers, internet networks, internet access points, district-issued accounts, storage, and district wi-fi.

D. **District technology resources:** means both district network resources and district-issued devices.

E. **"Privately-owned electronic device"** means a device, including an electronic device that is used for audio, video, text communication, or other type of computer or computer-like instrument that is not owned or issued by the District to a student, or employee. This includes, but is not limited to, cell phones, headphones/earbuds/airpods, and smartwatches.

F. **Technology protection measure**: A specific technology that blocks or filters Internet access to visual depictions, text, or other content that are obscene, pornographic, or harmful to minors and other inappropriate materials.

IV. PRIVILEGE OF USE AND MONITORING

A. The use of Weber School District's technology resources is a privilege, not a right.

B. No user has an expectation of privacy when using the district's technology resources.

1. The district has the right to monitor, inspect, review any and all usage of the district's technology resources.

2. The district reserves the right to monitor, store, access, and copy any student's files, activities, or communications, transmitted and received, at any time and without prior notice.

3. The district reserves the right to disclose to parents the contents of their student's files, activities, or communications, transmitted and received, and shall disclose contents as required by law. However, parents are not entitled to receive any and all content of their student's files, activities, or communications transmitted and received through the district's technology resources.

V. FILTERING AND INTERNET SAFETY

A. **Filtering Software**: The school system shall have in continuous operation a qualifying technology protection measure as defined in Policy 8330 and the Children's Internet Protection Act (CIPA). This includes monitoring online activities to protect against access to visual depictions, text, and other content that are obscene, pornographic, or harmful to minors and other inappropriate materials.

B. **Responsibility**: Students are responsible for their use of the district's technology resources and must avoid inappropriate materials. While technology protection measures are in place, it should not be assumed that users are completely prevented from accessing inappropriate materials or from sending or receiving inappropriate materials. Students who intentionally access, publish, or attempt to access or publish inappropriate material on district-owned devices or privately owned devices using district network resources will be subject to discipline, including temporary or long-term restrictions from district technology resources.

C. **Bypassing Filters**: Any efforts to bypass the district's technology protection measures or hide inappropriate online activity are prohibited and may result in discipline, including temporary or long-term restrictions from district technology resources.

D. **Reporting**: Students should notify the appropriate school authority if inappropriate material is encountered. Students must report to a teacher or principal immediately any sites with inappropriate material accessed by another student or accidentally accessed by the student.

VI. ACCEPTABLE USE OF DISTRICT OWNED DEVICES AND NETWORK RESOURCES

A. **Purpose**: Students are only allowed to utilize the district technology resources to retrieve information and run specific software applications as directed by their teacher, for legitimate educational purposes, including class work and independent research that is similar to subjects studied in school.

B. **Teacher Permission**: Students will only use district-owned devices with the teacher's permission and for the purpose the teacher requests. A teacher may restrict the use of district technology resources during class time using district provided software when necessary for instruction.

C. **Online Communication**: Any online communication using district network resources should always be at the direction and under the supervision of a teacher.

D. **Web Site Publishing**: When publishing on the Internet using district network resources, students must work under the guidance of a sponsoring teacher. Student participation in creation/maintenance of web pages requires logging onto the network with their own USER IDs and PASSWORDS.

VII. PROHIBITED CONDUCT. THE FOLLOWING IS PROHIBITED BY THIS POLICY

A. Creating, accessing, transmitting, or copying material or messages containing inappropriate material, including, but not limited to:

1. Obscene or pornographic content (including sensitive material, as defined in Policy 8250 and state law),

2. Inappropriate language and graphics, including swearing, vulgarities, sexually suggestive, belligerent, or abusive language of any kind

3. Hate speech, or materials promoting discrimination or violence based on race, ethnicity, religion, gender, sexual orientation, age, disability, or any other protected category

4. Harassment or bullying content, including cyberbullying in violation of Policy 5201, threats, or personal attacks, or inciting any of the above.

5. Violent or graphic content that is excessively disturbing or not instructional in nature

6. Content promoting illegal activity, including but not limited to drug use, underage drinking, solicitation of sexual material, selling stolen materials; vandalism, or hacking

7. Malicious software, phishing sites, or content attempting to compromise cybersecurity

8. Design or detailed information pertaining to explosive devices, criminal activities or terrorist acts;

9. Gambling; illegal solicitation; stolen materials; and commercial activities, including product advertisement.

B. Unauthorized Access/Use, including, but not limited to:

1. Using the network for financial gain or advertising; Attempting to read, alter, delete, or copy the email messages of other system users.

2. Using the school's computer hardware or district network resources for any illegal activity such as copying or downloading copyrighted software, music or images, or violation of copyright laws.

3. Downloading, installing, or using any other unauthorized program on any school computer or computer system.

4. Accessing entertainment sites, such as social networking sites or gaming sites, except for legitimate educational purposes under the supervision of a teacher or other professional.

5. Gaining access or attempting to access unauthorized or restricted network resources or the data and documents of another person.

6. Using or attempting to use the password or account of another person or utilizing a computer while logged on under another user's account.

7. Providing another student with user account information or passwords.

8. Using the school's computers or district technology resources while access privileges have been suspended.

9. Altering or attempting to alter the configuration of a school computer, district technology resources or any of the software unless explicitly allowed by a teacher for a specific course.

10. Attempting to vandalize, disconnect, or disassemble any district network resource or school computer component.

11. Connecting to or installing any computer hardware, components, or software which is not school system property to or in district-owned devices without prior approval of the district technology supervisory personnel.

12. Bringing on premises any disk or storage device that contains a software application or utility that could be used to alter the configuration of the operating system or network equipment, scan or probe the network, or provide access to unauthorized areas or data.

13. Downloading or accessing via e-mail or file sharing any software or programs not specifically authorized by Technology personnel.

14. Bypassing or attempting to circumvent district network security, virus protection, network filtering, or policies.

15. Possessing or accessing information on school property related to "hacking".

16. Purposely bringing on premises or infecting any school computer or district network resource with a virus, trojan, or program designed to damage, alter, destroy or provide access to unauthorized data or information.

16. Abusive use of the district network resources in any way that would disrupt network use by others; or the uploading, downloading or creation of computer viruses.

17. Impersonating the school district or any of its entities, employees, or students. This includes creating or using social media accounts, websites, email addresses, or any other digital content that falsely represents the school or utilizes district names, logos, or other intellectual property without explicit permission.

18. Installing or connecting any non-district-owned hardware, software, or peripheral devices to the district's technology infrastructure is strictly prohibited without prior written authorization from the Technical Services Department. This includes, but is not limited to, personal printers, external hard drives, monitors, and unauthorized software applications. Unauthorized modifications to district-owned technology are also forbidden.

19. Attempting to repair or contracting with external vendors to repair district devices is prohibited to ensure the integrity, security, and warranty of the equipment. All repair and maintenance of district-owned technology resources must be performed exclusively by authorized Technical Services personnel.

20. Using Virtual Private Networks (VPNs), proxy services, or any other technologies to circumvent district network security measures, content filters, or monitoring is prohibited. All network traffic on district-owned devices and within the district's network must remain transparent to ensure a safe and secure digital environment.

21. Engaging in political lobbying, including lobbying for student body office;

22. Using district technology resources to to cheat on school assignments or tests;

23. Transmitting communication through spam, chain letters, or other mass unsolicited mailings.

24. Sharing or posting personal information about or images of any other student, staff member or employee without permission from that student, staff member or employee.

25. Violating the district's rules for use of Artificial Intelligence as outlined in the WSD AI Framework.

26. Allowing or facilitating any of the above.

## VIII. USE OF PRIVATELY OWNED DEVICES

A. Students may not bring privately-owned electronic devices and connect them to the district network resources without using the appropriate password and access control, unless the student has express permission due to a health plan, a 504 plan, or an IEP.

B. If a student is allowed to connect their privately-owned electronic devices to district network resources, the student is prohibited from sharing any password and access control information with other students or staff.

## IX. SECURITY

A. **Passwords**: Students will only use their own passwords that have been given to them by the district. Students must protect passwords and never view, use, or copy others' passwords or share them. If a student suspects someone has discovered their password, they must change it immediately and notify their teacher or administrator.

B. **Storage Media**: Students are responsible for ensuring that any diskettes, CDs, memory sticks, USB

C. **Care for Equipment**: Students will respect the district-owned devices and take good care of the equipment used.

1. Students are prohibited from attaching anything on the district-owned devices for decoration or other purposes, including, but not limited to, stickers, beads, etchings, drawings, foil. This is considered vandalism and a student may be charged a fine.

2. Students are required to use a district provided charger to charge their district-owned devices. If a student loses their charger, the student must purchase a new one through the school.

3. Students are prohibited from inserting anything other than an approved computer peripheral (headphones, mouse, specialized keyboard, charging device, approved storage device).

## X. DISCIPLINARY ACTIONS

A. Violations of this policy may cause a student's access privileges to be revoked , other disciplinary action, and/or appropriate legal action to be taken. Inappropriate use may also result in disciplinary action (including the possibility of suspension or expulsion), and/or referral to legal authorities.

B. A student and their parents will be responsible for damages and will be liable for costs incurred for service or repair. The principal, teacher/supervisor, or systems administrator may limit, suspend, or revoke access to technology resources at any time for violations of this policy, which may result in missed assignments, inability to participate in required assessments, and possible academic grade consequences.

## XI. STUDENT AND PARENT ACCEPTANCE

A. Annually, within 45 days of each school year, a form containing the Technology Acceptable Use Policy will be included, along with the Bullying, Cyberbullying, Hazing, and Retaliation Policy, in the district's student information system, requiring parent and student acceptance. The combined signatures indicate the student and parent/guardian have carefully read, understand, and agree to follow the terms and conditions of appropriate use.