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 Educational System. 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. **CIPA (Children's Internet Protection Act)**: Federal regulations enacted by the Federal Communications Commission (FCC) and administered by the Schools and Libraries Division of the FCC

B. **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.

C. **Electronic device(s)**: A device used for audio, video, or text communication, or any other type of computer or computer-like instrument, including smartphones, smartwatches, tablets, or virtual reality devices.

D. **Inappropriate material:** any content—whether text, images, audio, video, or other digital media—that is not suitable for the school or district educational environment. This includes, but is not limited to:

1. Obscene, profane, or pornographic content (including sensitive material, as defined below)
2. Hate speech, or materials promoting discrimination or violence based on race, ethnicity, religion, gender, sexual orientation, age, disability, or any other protected category
3. Harassment or bullying content, including cyberbullying, threats, or personal attacks, or inciting any of the above
4. Violent or graphic content that is excessively disturbing or not instructional in nature
5. Content promoting illegal activity, including but not limited to drug use, underage drinking, vandalism, or hacking

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

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

8. Gambling; illegal solicitation; stolen materials; political lobbying; commercial activities, including product advertisement;

E. **Privately owned (device)**: A device, including an electronic device, used for audio, video, text communication, or other computer-like instrument, that is not owned, paid for, or issued by the district or individual school.

F. **Sensitive material**: Pornographic or sensitive material as defined in Utah Code Ann. § 76-10-1235(1)(a) and Utah Code Ann. § 53G-10-103.

G. **Technology protection measure**: A specific technology that blocks or filters Internet access to visual depictions that are obscene, child pornography, or harmful to minors.

IV. Privilege of Use and Monitoring The use of Weber School District's technology resources is a **privilege, not a right**. The district reserves the right to monitor, access, and disclose the contents of any student's files, activities, or communications. No user should have an expectation of privacy when using the district network or district-owned devices or equipment. The district has the right to monitor, inspect, copy, review, and store any and all usage of WSD technology resources including transmitted and received information at any time and without prior notice.

V. Filtering and Internet Safety

A. **Filtering Software**: The school system shall have in continuous operation a qualifying "technology protection measure" and procedures for monitoring online activities to protect against access to visual depictions that are obscene, child pornography, or harmful to minors.

B. **Responsibility**: Students are responsible for their use of the network and Internet and must avoid objectionable sites or materials. While filtering systems are in place, it should not be assumed that users are completely prevented from accessing inappropriate materials or from sending or receiving objectionable communications. Students who intentionally access, publish, or attempt to access or publish inappropriate or illegal material or Internet sites, will be subject to discipline.

C. **Bypassing Filters**: Any efforts to bypass the district’s internet and email filters or hide inappropriate online activity are prohibited.

D. **Reporting**: Students should notify the appropriate school authority if dangerous or inappropriate information or messages are encountered. Students must report any inappropriate sites observed being accessed by another user, or browsed to accidentally, to a teacher immediately. Students must report all security concerns, inappropriate activities, or misuse of Weber School District technology resources immediately to the principal, teacher/supervisor, or systems administrator.

VI. Acceptable Use of District Owned Devices and Network Resources

A. **Purpose**: Students are only allowed to utilize the computers and network 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 technology resources with the teacher's permission and for the purpose the teacher requests.

C. **Online Communication**: Any online communication should always be at the direction and with the supervision of a teacher.

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

VII. Prohibited Conduct (Includes, but is not limited to)

A. **Inappropriate Content/Communication**:

1. Accessing, sending, creating or posting materials or communications that are damaging to another person's reputation, abusive, obscene, sexually oriented, threatening or demeaning to another person, harassing, or illegal.
2. Contrary to the school's policy on harassment.
3. Never send, or encourage others to send abusive messages.
4. Use appropriate language and graphics; don't access, transmit, copy, or create material or messages that are threatening, rude, discriminatory, or meant to harass or cyber-bully. Swearing, vulgarities, suggestive, obscene, belligerent, or abusive language of any kind is not acceptable.
5. "Inappropriate material" includes, but is not limited to: design or detailed information pertaining to explosive devices, criminal activities or terrorist acts; pornography or indecent material; gambling; illegal solicitation; stolen materials; information used to cheat on school assignments or tests; commercial activities including product advertisement; political lobbying, including lobbying for student body office; online games (unless approved by supervising teacher as educational activity); illegal copies of copyrighted work; spam, chain letters, or other mass unsolicited mailings.
6. Never cyber-bully others; never post or send messages or pictures that hurt, threaten, or embarrass other people.
7. Participating on message boards without teacher direction, or in live chat using but not limited to AIM, Yahoo, or MSN Messenger.

B. Unauthorized Access/Use:

1. Using the network for financial gain or advertising; not buy or sell anything using the school's computers.
2. Attempting to read, alter, delete, or copy the email messages of other system users.
3. Using the school's computer hardware or network for any illegal activity such as copying or downloading copyrighted software, music or images, or violation of copyright laws.
4. Downloading, installing, or using games, music files, public domain, shareware, or any other unauthorized program on any school computer or computer system.
5. 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.
6. Gaining access or attempting to access unauthorized or restricted network resources or the data and documents of another person.

7. Using or attempting to use the password or account of another person or utilizing a computer while logged on under another user's account.
8. Providing another student with user account information or passwords.
9. Using the school's computers or network while access privileges have been suspended.
10. Altering or attempting to alter the configuration of a computer, network electronics, the operating system, or any of the software.
11. Attempting to vandalize, disconnect, or disassemble any network or computer component.
12. Connecting to or installing any computer hardware, components, or software which is not school system property to or in the district's technology resources without prior approval of the district technology supervisory personnel.
13. 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.
14. Downloading or accessing via e-mail or file sharing, any software or programs not specifically authorized by Technology personnel.
15. Bypassing or attempting to circumvent network security, virus protection, network filtering, or policies.
16. Possessing or accessing information on school property related to "Hacking", or altering, or bypassing network security or policies.
17. Exploring the configuration of the computer, operating system, or network, running programs not on the menu, or attempting to do anything not specifically authorized.
18. Purposely bringing on premises or infecting any school computer or network with a Virus, Trojan, or program designed to damage, alter, destroy or provide access to unauthorized data or information.
19. Abusive overloading of data on the server, use of the network in any way that would disrupt network use by others; or the uploading, downloading or creation of computer viruses.
20. Allowing or facilitating any of the above.

C. Privacy and Personal Information:

1. Never provide last name, address, telephone number, or school name online.
2. Giving out personal information such as phone numbers, addresses, driver's license or social security numbers, bankcard or checking account information.
3. Not sharing personal information about self or others like: home address, phone numbers, passwords, personal photos, or Social Security numbers.
4. Never send a photo of yourself or anyone else.
5. Never arrange a face-to-face meeting with someone met online.
6. Don’t distribute or post private information about yourself or others. This includes home address, personal phone numbers, last name of yourself or any other student, passwords, credit card numbers, student ID, or social security number.
7. Students may not share or post personal information about or images of any other student, staff member or employee without permission from that student, staff member or employee.

D. Copyright and Plagiarism:

1. Posting or plagiarizing work created by another person without his/her consent.

2. Not respecting copyright laws and not making sure to show where information was found, or copying it without permission.
3. Failing to give proper credit to all Internet sources used in academic assignments, whether quoted or summarized, including all forms of media.

E. Off-Campus Internet Expression: Maintaining or posting material to a Web site or blog that threatens a likelihood of substantial disruption in school, including harming or interfering with the rights of other students to participate fully in school or extracurricular activities. Students may be disciplined for expression on off-campus networks or websites only if the expression is deemed to cause a substantial disruption in school, or collide or interfere with the rights of other students, staff or employees.

VIII. Use of Privately Owned Devices

A. All student use of the District network and Internet system on personal cell phones or other digital devices while on campus is subject to the provisions of the individual school policies.
B. If a student is found to have abused a personal cell phone or digital device in a manner that is not in accord with this Appropriate Use Policy, the administrator may ban the student's use of any and all personal cell phone or digital devices.
C. The use of privately owned devices on school property or at school-sponsored events to access inappropriate matter, whether on district networks or personal data connections, is prohibited.
D. Students may not bring personal computers or hand-held computing devices and connect them to the school network or Internet connection (including connecting to wireless access points) without using the appropriate password and access control.

IX. Security

A. **Passwords**: Students will only use their own passwords that have been given to them by the teacher. 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 flash drives, or other forms of storage media they bring from outside the school are virus-free and do not contain any unauthorized or inappropriate files. Students will not put any disks or portable drives into the computer unless they are approved by the teacher.
C. **Care for Equipment**: Students will respect the technology resources and take good care of the equipment used.

X. Copyright and Plagiarism

- Students will respect copyright laws and will make sure to show where information was found and will not copy it without permission.
- Students are required to give proper credit to all Internet sources used in academic assignments, whether quoted or summarized. This includes all forms of media.
- Plagiarism of Internet resources will be treated in the same manner as any other incidences of plagiarism.

XI. Disciplinary Actions Violations of the Appropriate Use Guidelines may cause a student's access privileges to be revoked for a period of time up to one school year, other disciplinary action, and/or appropriate legal action to be taken. Inappropriate use may result in disciplinary action (including the possibility of suspension or expulsion), and/or referral to legal authorities. A student and his/her 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, which may result in missed assignments, inability to participate in required assessments, and possible academic grade consequences.

XII. Student and Parent Acceptance 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.

My Promise to Follow the Rules: I understand the importance of being polite, respectful, honest, and the need to obey the rules for the use of the computer, Internet, and other technology resources. If I break these rules, my principal or the District may take away my privilege to use the school's technology tools and I may have other disciplinary or legal action taken. I promise to follow the rules.