8310 Weber School District Staff Appropriate Use Policy

I. PHILOSOPHY

Weber School District provides technology resources for employees to enhance teaching and learning and to promote efficiency and excellence in the workplace by facilitating resource sharing, innovation, communication, cooperation, and collaboration. These resources include, but are not limited to, hardware, software, data, electronic textbooks and materials, electronic devices, printers, servers, filtered Internet access, AI, and local and wide area networks. This policy outlines the rules and guidelines for the acceptable use of these resources. All activities conducted using Weber School District technology resources are governed by this Agreement.

Use of these resources carries responsibilities. Employees are expected to use district technology in a lawful, ethical, and professional manner that upholds district values, protects student safety, and complies with applicable federal and state laws, including the Children's Internet Protection Act (CIPA). The district strictly prohibits the use of its technology resources for accessing, transmitting, or storing inappropriate, harmful, or illegal material; engaging in unauthorized or unlawful online activity; or disclosing personal identifying information of minors without authorization. The district reserves the right to monitor and review all activity conducted on its network and devices to ensure compliance with this policy and protect the integrity of its systems.

II. PURPOSE

The purpose of this Weber School District policy is to: (a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with the Children's Internet Protection Act 47 U.S.C. § 254(h), and Utah State Uniform School Code].

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, purchased, 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(s)**: 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, text, and other content that are obscene, child pornography, or harmful to minors.

IV. RESPONSIBILITY OF USE AND MONITORING

A. The District reserves the right to monitor, inspect, copy, review, access, and disclose the contents of any user's files, activities, or communications when using District-owned

devices or District networks. This includes any email, chat, or other electronic communication.

B. Employees do not have an expectation of privacy when using the District network or District-owned devices or equipment.

C. All documents created on District-owned devices are subject to public records disclosure laws.

V. FILTERING AND INTERNET SAFETY

A. **Filtering Software**: Filtering software is used on the district network to block or filter access to inappropriate material in accordance with CIPA. Technology protection measures shall be used to block or filter Internet access to inappropriate information, visual depictions of material deemed obscene, child pornography, or information harmful to minors. All Weber School District-owned devices shall have internet filtering software installed.

B. **Staff Responsibility**: Staff must be aware that students have access to the Internet from all of the district's computers. Despite filtering software, it is impossible to block access to all inappropriate material. Teachers are responsible for closely supervising their students' use of the Internet using district provided online monitoring tools. It shall be the responsibility of all members of the Weber School District staff to supervise and monitor usage of the online computer network and access to the Internet in accordance with this policy and CIPA.

C. **Bypassing Filters**: Any efforts to bypass the district's internet and email filters or hide inappropriate material are prohibited, including proxies, special ports, altering browser settings, or any other methods aimed at evading filters or accessing/sharing inappropriate material. Any attempt to disable or bypass filtering software is a violation of this policy..

D. **Reporting**: Employees should notify the appropriate school authority if dangerous or inappropriate material or messages are encountered. Employees must report all security concerns, access to inappropriate materials, or misuse of Weber School District technology resources immediately to the principal, supervisor, or systems administrator. This includes the receipt of messages relating to or in support of illegal activities or that may be threatening or upsetting.

VI. ACCEPTABLE USE OF DISTRICT-OWNED DEVICES AND NETWORK RESOURCES

A. **Purpose**: District-owned technology resources are provided primarily for legitimate educational and business purposes that promote and are consistent with the instructional goals and operations of the Weber School District.

B. **Professional Conduct**: Employees should model the behavior expected of students.

C. **Email Communication**: Email accounts are provided for professional purposes.

1. All employee communications with parents students must be through district-issued email accounts or district-approved software.
2. Emails to parents, students, and colleagues should be carefully constructed to ensure compliance with FERPA.
3. Email communications are subject to public records request and/or litigation.
4. Personal emails may not be sent through district-issued accounts.
5. Personal email accounts should not be used for work purposes.
6. Employees must request permission from the building administrator before sending any messages to a public official from a district-issued email account.
7. Sending emails to a public official from a personal account is NOT prohibited by this policy.

D. **Web Site Posting**: All material posted must be educationally sound and appropriate, and must comply with Policy 7340 Employee Social Media Policy

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

A. Prohibited 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, accessing, transmitting, copying, or creating material or messages that are threatening, rude, discriminatory, or meant to harass or cyber-bully. or
2. Swearing, vulgarities, suggestive, obscene, belligerent, or abusive language of any kind.
3. Accessing inappropriate material, whether on or off district property on a district-owned device or district network.
4. Illegal activities, or transmission or intentional receipt of any inappropriate material in violation of law or WSD policy.

B. Unauthorized Access/Use:

1. Using the network, district-provided hardware, and district-provided platforms and/or licenses for financial gain or advertising.
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.
4. Downloading, installing, or using games, music files, public domain, shareware, or any other unauthorized program on any school computer or system.
5. Accessing entertainment sites, such as social networking sites or gaming sites, except for legitimate educational purposes.
6. Gaining access or attempting to access unauthorized or restricted network resources, or the data and documents of another person, including any other so-called “hacking” activities.
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 user 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 standard configuration of a computer, network electronics, the operating system, or any of the software.
11. Attempting to vandalize any network or computer component.
12. Attempting to disconnect or disassemble any network or computer component without technology department oversight and authorization.
13. Connecting to or installing any computer hardware, components, or installing software on school devices without prior approval of the district technology personnel.
14. Purposely bringing on premises, or infecting any school computer or network with, a virus, or program designed to damage, alter, destroy, or provide access to unauthorized data.
15. Abusive overloading of data on the server or use of the network in any way that would disrupt network use by others.
16. Spreading email chain letters, mail bombs, virus hoaxes, Spam mail.
17. Allowing students to log in with a staff member's user name and password.
18. Allowing a student to use a computer unless they are logged on under their own name.
19. Allowing students to go to computer labs unsupervised.

C. Privacy and Personal Information:

1. Giving out others' personal information obtained in the course and scope of employment such as home address, personal phone numbers, passwords, credit card numbers, student ID, social security number, driver's license or, bankcard or checking account information on district-owned or privately-owned devices or accounts.

2. using district-owned devices, accounts, or network.

3. Electronically sharing or disclosing education records or employee financial, health or other personnel records with other employees, parents, or students without express written permission or without an educational or employment need to know.

VII. USE OF PRIVATELY OWNED DEVICES

A. The use of privately owned devices on school property or at school-sponsored events to access pornographic or indecent material as defined in Utah Code 76-10-1235, whether on district networks or personal data connections, is prohibited.

B. Privately owned electronic devices may use designated WiFi networks and the internet system at the discretion of Technical Services. Connectivity may be restricted or terminated without notice.

C. Privately owned electronic devices shall, under no circumstances, be connected to the district's wired network and Internet systems.

VIII. SECURITY

A. **Passwords**: Any employee issued a password is required to keep it private and not permitted to share it. Employees are required to change passwords periodically. Employees must not allow students to look over their shoulder and have access to password information.

B. **Data Storage**: Users are responsible for the appropriate storage and backup of their data downloaded directly to a device.

C. **Unauthorized Software/Hardware**: Employees are not permitted to connect or install any computer hardware or components which are not school system property to or in the district's technology system without prior approval of Technical Services.

X. DISCIPLINARY ACTIONS

A. Violations of this Appropriate Use Policy may result in corrective action (including warning, reprimand, probation, or suspension), and/or appropriate legal action, up to and including employment termination. If appropriate, violations may be reported to law enforcement.

XI. EMPLOYEE ACCEPTANCE

A. I have read this Acceptable Use Agreement and agree to comply with the conditions of acceptable use and to report any misuse of Weber School District technology resources to the appropriate administrator. I understand any violations of the above provisions may result in the loss of use of Weber School District technology resources and may result in further disciplinary action, including but not limited to, termination, and/or referral to legal authorities.