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.

II. POLICY

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.

III. DEFINITIONS

A. "District Technology Resources" means district-issued owned devices, district network resources, and district-issued accounts and logins.

B. "District-owned Device(s)" means 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. This includes but is not limited to:

1. Desktop Computers (also called "school computers")
2. Chromebooks
3. Computer peripherals (keyboards, mice, headsets, etc)
4. iPads
5. Laptops
6. Display panels

C. **"**District Network Resources" means District-owned network technology, including but not limited to:

1. servers,
2. internet networks,

3. network wiring

4. internet access points,

D. "District Issued Accounts and Logins" means District provided access to Google for Education and other purchased and approved software and programs.

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. "Inappropriate material" means any content—whether text, images, audio, video, or other digital media—that is not suitable for the school or district educational environment.

G. "Technology protection measure" means a specific technology that blocks or filters Internet access to visual depictions, text, or other content that is obscene, pornographic, or harmful to minors and other inappropriate materials.

IV. MONITORING AND PRIVACY

A. No user has an expectation of privacy when using the district's technology resources. The district has the right to monitor, inspect, and review any and all usage of the district's technology resources.

B. Privately-owned staff electronic devices connected to the district network are filtered, but not monitored. Employees using a privately-owned electronic device and a personal account or software, not a district provided account or software, will not be monitored in their use of their personal account or software.

V. FILTERING AND INTERNET RESPONSIBILITY TO MONITOR

A. Filtering Software

1. In accordance with CIPA and Policy XXX, 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.

2. Any efforts by employees 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.

B. Responsibility to Monitor Students

1. 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.

2. Employees must report to the district's Technical Services Department immediately any sites with inappropriate material accessed by a ~~another~~ student, either intentionally or accidentally. ~~or accidentally accessed by the student.~~

VI. ACCEPTABLE USE OF DISTRICT TECHNOLOGY RESOURCES

A. Purpose: District 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. Except as outlined in VI.B. below, employees may use District technology resources for personal matters in addition to the primary purpose of fulfilling the employee's duties as a public employee so long as it does not interfere with the employee's duties and responsibilities.

B. 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 about work-related matters (whether on personal or work email accounts), and emails from district-issued accounts (whether about personal or work-related matters) are subject to public records request and/or litigation.

4. Personal email accounts should not be used for work purposes.

5. Work email accounts shall not be used for personal purposes.

6. Employees must request permission from the building administrator before sending any messages to a public official from a district-issued email account. Sending emails to a public official from a personal account is NOT prohibited by this policy.

7. Employees may not transmit communication through spam, chain letters, or other mass unsolicited mailings.

D. Web Site Posting: All material posted to district or school websites must be up-to-date, educationally sound, and appropriate.

E. Social Media:

1. All social media postings related to students and/or duties and activities as a district employee must comply with Policy 7340 Employee Social Media Policy.

2. All material posted to district or school social media accounts must be up-to-date, educationally sound, and appropriate.

3. School and district social media account logins may not be shared with students and students are prohibited from posting on school and district social media accounts.

VII. PROHIBITED CONDUCT. **The following is prohibited by this policy:**

A. Using district technology resources, employee may not create, access, transmit, or copy, 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, 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

   8. malicious software, phishing sites, or content attempting to compromise cybersecurity

   9. design or detailed information pertaining to explosive devices, criminal activities or terrorist act;

   10. gambling; illegal solicitation; stolen materials; and commercial activities, including product advertisement.

B. Employees may not engage in unauthorized access or use of district technology resources, including, but not limited to:

   1. using the network 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 district network resources for any illegal activity such as copying or downloading copyrighted software, music or images, or violation of copyright laws.

   4. downloading, installing, or using any other unauthorized program on any school computer or computer system.

   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 a student with user account information or passwords.

   8. altering or attempting to alter the configuration of a school computer, district technology resources or any of the software unless explicitly allowed by Technical Services for a specific course.

   9. attempting to vandalize, disconnect, or disassemble any district network resource or school computer component.

   10. connecting to or installing any computer hardware, components, or software which is not district-owned without prior approval of the Technical Services Director.

11. bringing on premises any 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.

12. downloading or accessing via e-mail or file sharing, any software or programs not specifically authorized by Technical Services.

13. bypassing or attempting to circumvent district network security, virus protection, network filtering, or policies.

14. possessing or accessing information on school property related to "hacking" or altering, or bypassing network security or policies.

15. 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 (including printers) 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 (this does not apply to privately owned devices and personal accounts while off contract time)

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

23. allowing or facilitating any of the above.

VIII. 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 District WiFi networks. 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.

D. A privately owned devices may only be used by the employee who purchased the device while on the district network and may not be used by other employees or students.

IX. SECURITY

A. Passwords:

1. All employees are required to keep their district passwords private and are not permitted to share them with anyone.
2. Employees are required to change passwords periodically.
3. Employees must not knowingly allow students access to password information.

B. Multi-Factor Authentication

1. Multi-factor authentication is required for all employees when using district technology resources.
2. Employees may install multi-factor authentication on a personally owned device or may request a district-owned faub for this purpose.

C. Data Storage: Employees are responsible for the appropriate storage, backup, and transfer of their personal and work data downloaded directly to district-owned devices.

D. Data Storage on a Privately Owned Device. Employees assume full and sole liability for the protection of any district data, including employee and student information, that they choose to store on a privately owned device. Should a data breach occur originating from the device, the liability for that breach will fall upon the employee as the owner.

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.