7145 DISTRICT PERSONNEL ELECTRONIC DEVICE POLICY - New Policy

I. PURPOSE AND PHILOSOPHY

Weber School District, hereinafter referred to as "District" and "WSD", promotes an environment conducive to teaching and learning. The District recognizes that electronic devices are valuable tools for instruction and communication. Additionally, the District recognizes that electronic devices may become sources of disruption and may pose safety and privacy issues.

II. PROCEDURE

In order to maintain an effective learning environment, and to promote safety and security, the District adopts this Policy governing District personnel's use of electronic devices, as required by Utah School Board Rule 277-495. This policy shall act in conjunction with Policy 8311 Appropriate Use Policy for Computers and Network Resources; Policy 8310 - Appropriate Use Policy for Employees; and 8300 - Internet Safety Policy.

III. DEFINITIONS

A. "Appropriate use policy" means a document stipulating constraints and practices that a user shall accept prior to a user accessing the District's, or any school within the District's, network or the internet.

B. "District-owned electronic device" means a device that is used for audio, video, text communication, or other type of computer or computer-like instrument that is identified as being owned, provided, issued, or lent by the District to an employee.

C. "Electronic device" means a device that is used for audio, video, or text communication or any other type of computer or computer-like instrument including:

1. a smart phone;
2. a smart or electronic watch;
3. a tablet; or
4. a computer, desktop, and laptop.

D. "Employee" means an individual working in the individual's official capacity as a teacher; school staff member; school administrator; district administrator; district staff member; or governing board member.

E. "Government Records Access Management Act ("GRAMA") is a law that allows for the release of government documents at the request of an individual. A GRAMA request can be made to the District for electronic documents/communications stored

or transmitted through District systems unless that information could be detrimental to governmental or personal interests. UTAH CODE ANN. § 63G-2- 101 et seq.

F. "Guest" means an individual/user:

1. who is not a student, employee, or designated volunteer of a public school; and

2. who is on school property or at the site of a school-sponsored activity or event.

G. "Inappropriate matter" means pornographic or indecent material as defined in Utah Code Ann. §76-10-1235(1)(a).

H. "Incidental personal use" means use of a District-owned electronic device or privately-owned electronic device on the District's network by an individual employee for personal communication and information.

I. "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 an employee.

V. DISTRICT PERSONNEL RESPONSIBILITIES REGARDING DISTRICT-OWNED ELECTRONIC DEVICES

A. Employees who are issued District-owned electronic devices, are responsible for said devices at all times and any misuse may be subject to disciplinary actions, regardless of the user.

B. The entirety of section V of this Policy, applies to all District-owned electronic devices, regardless of proximity to District property or connectivity to the District's network/servers.

C. All communication sent by an employee using District property or regarding District business could be subjected to public access requests submitted through the GRAMA. By agreeing to use District-owned electronic devices and/or District networks, employees acknowledge that data and other material/files maintained on the District's systems may be subject to review, disclosure, or discovery.

1. Use of personal email accounts and communication tools to conduct District business is strongly discouraged and may open an individual's personal account to be subject to GRAMA inquiries.

2. The employee may be required to disclose the content in response to a subpoena, court order, discovery request, or request for records under GRAMA.

3. In addition, the District may require disclosure to investigate allegations of misconduct.

VI. PROHIBITED USES

A. The following prohibited uses of electronic devices applies to all District-owned and privately-owned electronic devices that are on District property, at a District-sponsored event, and/or are connected to District networks or District systems:

1. Electronic devices are prohibited from being used in ways that:

    i. bully (including cyberbullying), humiliate, harass (including sexual harassment), or intimidate school-related individuals, including students, employees, and guests;

    ii. violate local, state, or federal laws;

        a. attempting unauthorized access (e.g. hacking, altering, or bypassing network security), and/or

        b. dissemination of personal student information under the Family Educational Rights and Privacy Act (FERPA) 34 CFR, Part 99.

    iii. invade reasonable expectations of privacy of school-related individuals, including students, employees, and guests.

        a. Electronic devices with the capacity to record, stream, or otherwise transmit images or audio may not be used at any time in any school location where a reasonable expectation of personal privacy exists.

            1. These locations and circumstances include, but are not limited to, locker rooms, shower facilities, restrooms, and any other areas where students or others may change clothes or be in any stage or degree of disrobing or changing clothes.

    iv. disrupt the educational environment including instructional time spent on District-owned and privately-owned electronic devices;

    v. conduct unethical activities; and

    vi. disseminate information deemed inappropriate matter (e.g. sexting).

2. District employees are prohibited from accessing inappropriate matter on the internet while using District-owned electronic devices, services, or networks whether on or off District property.

    i. The use of electronic devices to access inappropriate matter on District-owned electronic devices or privately-owned electronic devices on District property, at school-sponsored events, or using District networks will be subject to employee disciplinary action, and when appropriate, may be reported to law enforcement for criminal action.

VII. CORRECTIVE ACTION

A. Any violation of this Policy will be referred to the employee's supervisor and Human Resources to be addressed pursuant to Policy 7900 - Suspension or Termination of District Employees and Corrective Action.

1. Corrective actions shall be in accordance with applicable laws, regulations, and District policies.

2. Any employee found to be in violation of this Policy may be subject to corrective action up to and including termination of employment with Weber School District.

B. Weber School District will cooperate fully with local, state, and federal authorities in any investigation concerning or related to any illegal activities or activities not in compliance with District policies or government regulations.

VIII. NO EXPECTATION OF PRIVACY

A. The District retains control, custody, and supervision over all District-owned electronic devices and network services owned, licensed, or leased by the District.

B. The District reserves the right to access, monitor, review, copy, store, or delete any files (unless other restrictions apply) stored on District-owned electronic devices and all employee communication using the District's network and may occur without notice to employees.

1. Electronic messages and data stored on WSD devices or transmitted using WSD network/systems may be treated like any other District property.

2. District administrators and personnel may review files and messages to maintain system integrity and, if necessary, to ensure that users are acting responsibly.

3. WSD may choose to deploy location tracking software on devices for the sole purpose of locating devices identified as lost or stolen.

C. By utilizing District-owned electronic devices and the District's network services, employees acknowledge that they have no expectation of privacy.

D. Employees are to utilize District-owned electronic devices and network services for the performance of job duties and professional or career development activities.

E. Incidental Personal Use

1. Employees who conduct incidental personal use on District-owned electronic devices and network services acknowledge that the incidental personal use may be subject to inspection and therefore waive any expectation of privacy. Incidental personal use is permitted as long as such use does not interfere with:

i. the employee's job duties and performance;

ii. computer system operations; and/or

iii. other computer system users.

2. Employees acknowledge that any incidental personal use shall comply with this Policy and all other applicable policies and administrative procedures, directives, and rules.

IX. RISK OF LOSS

A. Employees shall take reasonable measures to prevent District-owned electronic devices and privately-owned electronic devices from being lost or stolen.

1. In the event an electronic device is lost or stolen, an employee shall immediately notify appropriate staff, their direct supervisor, local authorities, and/or the Technical Service Department.

B. WSD will take reasonable measures to attempt to recover the lost property.

C. WSD is not responsible for the security or safekeeping of privately-owned devices and is not financially responsible for their loss, theft, and/or damage.