Originally Adopted: Policy 532, January 2015 Revised/Reformated: _____

FAB STUDENT ELECTRONIC DEVICE POLICY

Purpose

—

The District supports the use of technology to enhance and support learning, recognizes the value of students using both district provided and privately owned electronic devices, and allows students and others the rights and responsibilities of using these devices on district property.

References-

The Children's Internet Protection Act (CIPA)

Family Education Rights and Privacy Act (FERPA)

Utah Administrative Code Ann. R277-495 Electronic Devices in Public Schools

Definitions—

The following definitions apply to this policy:

1. "User" means anyone, including employees, students, and guests, using an electronic device.
2. "Network" means any wired or wireless system that allows for the exchange of data, including school and district networks, cellular networks, commercial, community, or home-based wireless networks accessible to students.
3. "Device" means electronic equipment that sends, receives, or stores data. Examples include but are not limited to: mobile or smart phones; MP3 players, iPods, portable gaming equipment; portable computers such as laptops, iPads, tablets, web thin clients (e.g., Chromebooks), netbooks, and wearable technology; as well as portable storage devices such as hard drives, flash drives, SD Cards, and

Micro Drives.

4. “Responsible Use Policy (RUP)” means the district policy that delineates appropriate use of the Internet or other electronic information resources.
5. “Privately Owned Device” means a non-district supplied device used during school, on district property, or at district sponsored events.
6. “Electronic Information Resources” include, but are not limited to, the Internet, digital curriculum, texts, email, chat rooms, blogs, and other network files or accounts available to students.
7. “Reasonable or Reasonably” means efforts by administration, school staff, or law enforcement to prevent: disruption to instruction or other school sponsored activities, damage to school or district property, or interference with school operations within the confines of current state or federal law, school rules, or district policies.

Policy

—

Students have the privilege of using electronic devices on district property or at district sponsored events pending:

1. Receipt, understanding, and willingness to adhere to this policy, and the district’s Responsible Use Agreement deemed appropriate by the school district for each student’s current age or ability level.
    a. Use agreements are signed annually or as soon as reasonably possible after an update is adopted.
    b. Use agreements are to be stored in a manner and location where they may be verified by administration or law enforcement when needed. c. Use agreements are reviewed for possible updates at least every three years.
2. Receipt, understanding, and willingness to adhere to rules and procedures developed at the school the student attends and by individual classroom instructors to regulate the use of electronic devices.
3. Students violating policy or school rules may be required to complete district sponsored training activities specific to the policy or school rules violated.
4. Building administrators and district technology staff may search a student’s device memory when reasonable suspicion exists that a state or

federal law, district policy, or school rule has been violated.

5. Building or district administration will turn over a confiscated device to law enforcement for initial or additional searches when reasonable suspicion exists that the device was used in violation of state or federal law.

6. Violations of law will result in referral to law enforcement for possible criminal prosecution as well as disciplinary action by the District.

7.Students may use audio recording devices, cameras, video recording devices, messaging devices, or any device with data capture or communication capabilities unless otherwise reasonably directed by administration, law enforcement, a staff member or those who are being recorded or about whom information is being shared.

8. Unless otherwise reasonably directed by administration, law enforcement, a staff member, or those who are being recorded or about whom information is being shared, students may share audio, images, video, or any form of electronic communication with the exception of audio and video recordings, photographs, or electronic communications that violate reasonable expectations of privacy, current law or district policy, or other issues including bullying, harassment, intimidation, interference with school operations, disrupting school activities, etc.

Privately Owned Devices

Students have the privilege of using privately owned electronic devices in compliance with state and federal law, district policy, and school and classroom rules.

Building administrators and district staff may confiscate a privately-owned device if federal or state law, district policy, or school or class rules are violated.

Building administrators or district technology staff may search a privately-owned device, when the use of the device most likely involved the school network or school district resources to violate the law.

When a confiscated device is privately-owned and the school network or school district resources were not likely involved in the suspicious activity the device will be turned over to law enforcement for initial or subsequent investigation(s) involving state or federal law.

Enforcement

Confiscatio
n

If a student violates this policy, his/her electronic device may be confiscated.

When an employee confiscates an electronic device under this policy, he/she shall take reasonable measures to label and secure the device and turn the device over directly to a school administrator or administrative designee as soon as the employee's duties permit.

The electronic device will be released/returned to the student or student's parent or guardian after the student has complied with any other disciplinary consequence that may be imposed.

Investigations

School and/or district administration, in consultation with district technology staff as needed, shall determine whether to investigate and/or make a referral to law enforcement for investigation in accordance with current state and federal law. School administration and/or law enforcement may search school district issued devices, as well as, privately owned devices using the school district's network for activities suspected of violating this policy.

School administrations and/or law enforcement may search school district created accounts and applications, as well as, private accounts or applications accessed through the school district's network for activities suspected of violating this policy.

Privately owned devices, private accounts, or private applications used on school property or at school sponsored events suspected of violating state or federal law will be referred to law enforcement for investigation when the district network was clearly not involved in the use of the device, account or application.

Disciplinary Actions

Violation of this policy may result in disciplinary actions up to and including the following:

1. Suspension in or out of school, or expulsion.

2. Notification of law enforcement authorities.

3. Permanent prohibition from possession of an electronic device at school or school-related events, and only supervised, temporary access to an electronic device for instruction as deemed necessary by an instructor or school tutor.

4. Confiscation of device for increasing periods of time for repeat violations,

5. Other disciplinary actions as deemed appropriate by school administration.

Access to District Wireless Network

Access to the district wireless network, including the internet, is permitted primarily for instructional purposes and is a privilege not a right. Limited personal use of the district wireless network is permitted if the use:

1. Imposes no tangible cost to the District.
2. Does not unduly burden or cause damage to the district's computer or network resources.
3. Has no adverse effect on a student's academic performance.

Students using the district network agree to:

1. Abide by all state and federal laws.
2. Use the internet primarily for education and instruction.
3. Conduct themselves in a responsible, decent, ethical, and polite manner.
4. Accept the responsibility for adhering to high standards of personal digital citizenship to ensure quality network access for all users expected in school environments.

The District is not responsible for the ability of privately-owned devices to access the district network. Guidelines for accessing the district network with privately owned devices may be obtained by reviewing information provided through the district website or by contacting district technology department personnel.

Authentication

Personal and device information may be required when accessing the district network to access district electronic resources or the internet. Information may include, but is not limited to: name, email, student identifications (where applicable), passwords, phone numbers, device credentials (e.g., IP Address), etc.

Device Requirements

OS, phone, tablet, laptop, and other systems supported by the District may be found through the district website or by contacting district technology department personnel. Network authentication processes are configured to support secure and safe data exchanges with district owned devices for educational purposes.

Filtering

All devices accessing the district network on or off of district property will have content filtered in accordance with federal and state law, including, compliance with the Children's Internet Protection Act (CIPA) and the Family Education Rights and Privacy Act (FERPA).

District provided devices and privately-owned devices accessing the district network or its resources may be required to allow device management as specified by the district technology department.

The District claims no liability for filtering related to use of privately-owned devices or district provided devices on home networks or other networks not provided by the District, even when access is for school related activities or assignments.

Homeowners and other access providers are responsible for their own filter configurations and cannot be monitored or supported by the District.

The District reserves the right to investigate the use history, downloads, or drives for any device accessing the district network, even when the use history, downloads, or drive configurations occurred on a non-district provided network.

File Storage and Access

The District provides access to electronic storage for educational purposes, including, but not limited to all supported electronic media, electronic curriculum, resources, etc.

District storage resources are available for secure access and protection of student and staff educational work and records.

District technology staff will follow current best practices for protecting staff and student files and data, including but not limited to: firewall maintenance, annual penetration testing, secure server facilities, redundant back up, recovery systems, etc.

Power

The District provides some access to power to support the use of technology for educational activities. The District is under no obligation to provide access to power for all devices in use during instruction or other school or district sponsored activities.

Those using devices on campus are expected to make reasonable preparations to fully power devices before coming to campus for educational, instructional, or other school or district sponsored activities.

Students, may access power freely on district power sources unless otherwise directed by administration or sponsors of district or school activities.

Liability

Lost, Stolen, or Damaged Devices

Devices are the responsibility of the private owner or the assigned user, and each user, private or assigned, should use best practices to preserve the device life and full operating condition.

Logan City School District takes no responsibility for stolen, lost, or damaged devices, including lost or corrupted data on those devices.

Private owners or assigned users are responsible for knowing best practices for keeping a device secure, and are solely responsible for securing privately owned or assigned devices.

An employee or designee of the District responsibly handling a privately owned device or a device assigned to another user, during the course of his or her duties, shall not be responsible for stolen, lost, or damaged devices, including lost or corrupted data on those devices.

Usage Charges and Cyber Theft

Logan City School District and its employees are not responsible for any device charges to private credit, online, or other accounts that might be incurred during approved school related use.
Logan City School District and its employees are not responsible for any device charges resulting from non-school related use of a device.

Logan City School District and its employees are not responsible for cyber theft resulting from the use of devices under any circumstances.

Examples include but are not limited to cyber theft occurring: from a device supplied by the school district, from a privately-owned device while on school district property, while participating in a school or district sponsored activity, while using the school district network, while using a private network, etc.