Replaces: 531 adopted in 2015
Adopted: February 11, 2020

FEF

Student Responsible Use of the Internet and Other Electronic Information Resources

Purpose—
The District supports access to and the responsible use of information and communications technology (ICT) to enhance and support learning. The District strongly believes that the valuable information and interactions available through information and communication systems, are effective ways to connect students to the growing global information resources needed for their education and therefore necessary in learning environments.

References—
The Children's Internet Protection Act (CIPA)
Family Education Rights and Privacy Act (FERPA)
Utah Code Ann. § 76-10-1235(1)(a) *Accessing pornographic or indecent material on school property*
Utah Admin. Rules R277-495-4(1)(b) (April 8, 2019)
Logan City School District—FAB Student Electronic Device

Definitions—
"User" means anyone, including employees, students, and guests, using an electronic device.
"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.
"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.
"Responsible Use Policy" (RUP) means the district policy that delineates appropriate use of the Internet or other electronic information resources.
"Privately Owned Device" means a non-district supplied device used during school, on district property, or at district sponsored events.
"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 users.
"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—

The District and the Utah Education Telehealth Network (UETN) have taken available precautions to restrict access to objectionable materials and unauthorized access to individual data associated with information and communication systems.

The District holds individual users responsible for personal activity with information and communication systems provided by the District, including the discovery of controversial or inappropriate information not prevented by the efforts of District and UETN personnel.

Individuals using district networks or information and communication systems are monitored and should have no expectation of privacy.

Student Responsible Use

Students have the privilege of accessing district information and communication systems on and off district property pending:

1. Receipt, understanding, and willingness to adhere to this policy, and the district's Electronic Device Policy.
2. Receipt, understanding, and willingness to adhere to the Responsible Use Agreement deemed appropriate by the District for each student's current age or ability level.
3. Use agreements are:
    a. Signed annually.
    b. Stored in a manner and location where they may be verified by administration or law enforcement when needed.
    c. Reviewed for possible updates at least every three years.

Appropriate Use of an Electronic Device:

- Abides by all state and federal laws
- Is conducted in a responsible, decent, ethical, and polite manner
- Has no adverse effect on a student's academic performance
- Adheres to high standards of personal digital citizenship
- Imposes no tangible cost to the District
- Does not unduly burden or cause damage to the district's computer or network resources

Examples of inappropriate use include, but are not limited to accessing or disseminating information construed by the District as: profane, obscene (pornographic), violent, discriminatory, harassment, bullying, intimidating, or advocating illegal acts.

Investigations

- School and/or district administration, in consultations 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:

- Blocking or reducing the level of student access to the district wireless network
- Suspension in or out of school, or expulsion
- Notification of law enforcement authorities
- 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 a staff member
- Confiscation of device for increasing periods of time for repeat violations,
- Other disciplinary actions as deemed appropriate by school administration

Student Due Process

1. If there is an allegation that a student has violated this policy, the student shall be referred to the appropriate school authority, receive notice of the alleged violation, and provided an opportunity to present an explanation.
2. In the event an allegation may lead to disciplinary action, the investigating school official or designee shall inform parents of the allegation and potential disciplinary action.
3. Disciplinary actions in harmony with the school handbook will be tailored to meet the specific concerns related to the violation.
4. Deliberate violations of this policy (e.g., malicious acts or omissions; searching for, viewing, or otherwise visiting pornographic or sexually explicit sites) are cause for suspension or expulsion for students.

Student Access Through Private Networks
Students using private networks to access content or to communicate while on district property or at district sponsored events are held to the same expectations as if they

were using the district network. School officials will discipline students using private networks to violate district policy, school rules, or classroom rules. Students using private networks to violate federal or state law will be referred to appropriate law enforcement agencies for investigation or prosecution.

Student Access to the 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:

- Abides by all state and federal laws
- Imposes no tangible cost to the District
- Does not unduly burden or cause damage to the district's computer or network resources
- Has no adverse effect on a student's academic performance
- Is conducted in a responsible, decent, ethical, and polite manner
- Adheres to high standards of personal digital citizenship to ensure quality network access for all users expected in school environments.

The District makes no warranties of any kind, whether express or implied, for services provided and is not responsible for any damages suffered while on the system to include loss of data and inaccurate or poor-quality information obtained from the system.

Enforcement
If a student violates this policy, his/her access to the district network may be blocked or reduced.

- The level of student access will be tailored to the circumstances surrounding the violation based on parent, staff, and/or administrator input and the capabilities of the current district information and communication system
- Removing limited or blocked access will be depend on student compliance with all other aspects of the Responsible Use Agreement as well as recommendation of parents, staff, and/or administration requesting the restriction

Authentication
The District claims the right to manage all network activity of individuals accessing or authenticating onto district information and communication systems, including but not limited to:

- Verifying personally identifiable information (PPI)
- Gathering data on use for policy enforcements
- Gathering PPI data for administrative purposes related to the network

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.

Network authentication processes are configured to support secure and safe data exchanges with district owned devices for educational purposes.

Filtering
When authenticating onto the district network on or off of school district property:

- Content will be 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)
- 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
- 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

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

- Users are responsible for storage and security of personal files unrelated to educational activities
- Personal storage requirements exceeding or inhibiting device capacity and use should be maintained through other storage options and not on the device.
- Educational files should be secured and accessed through district storage resources

Training—
All staff will be trained in current responsible use policy annually, and as soon as reasonably possible after a change in state or federal law, school rules, or district policy.
Students will be trained by staff or required to complete district sponsored training sessions at least annually, including but not limited to: Internet safety and digital citizenship, authentication policy and procedures, and file storage and data management.
Students violating policy or school rules may be required to complete district sponsored training activities specific to the policy or school rules violated.

Liability—

Lost, Stolen, or Corrupted Files

Personal and educational files are the responsibility of the user and users are encouraged to follow best practices to preserve files. Logan City School District takes no responsibility for stolen, lost, or corrupted files, and encourages regular backup of both personal and educational files.

Usage Charges and Cyber Theft

Logan City School District and its employees are not responsible for:

- Any charges to private credit, online, or other accounts that might be incurred during approved school related use
- For cyber theft resulting from inappropriate sharing of personal login or authentication information under any circumstances.

Examples include but are not limited to: sharing district provided user names or passwords, sharing a personal user names or passwords through the district network, etc. that are then used for cyber theft.