The Center for Creativity, Innovation and Discovery
Responsible Electronic Device Use Policy

Purpose
The Center for Creativity, Innovation and Discovery ("CCID") supports the use of technology to enhance and support learning, recognizes the value of the students using both CCID-provided and privately owned electronic devices, and allows students and others the rights and responsibilities of using these devices on CCID property.

References
Examples of federal law, state law, and industry standards include, but are not limited to, the following:

- **Children's Internet Protection Act** (CIPA)
- **Federal Educational Rights and Privacy Act** (FERPA)
- **Utah Code Ann. § 53A-3-422** Internet and Online Access
- **Utah Code Ann. §53A-1-402.5** Employee Ethical Conduct

Definitions

- *User:* anyone, including employees, students, and guests, using an electronic device.
- *Network*: 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*: 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 Microdrives.
- *Responsible Electronic Device Use Policy* (RUP): CCID's policy that delineates appropriate use of the Internet or other electronic information resources, formerly known as the Acceptable Use Policy.
- *Privately Owned Device*: 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 students.
- *Reasonable or Reasonably:* 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.

Conditions of Use

I. General Terms of Use.

II. Students have the privilege of using electronic devices on CCID property or at CCID-sponsored events pending acceptance of the following terms and under the following circumstances:

- Receipt, understanding, and willingness to adhere to this policy and the *Responsible Use Agreement*
- Receipt, understanding, and willingness to adhere to rules and procedures of the school and individual classroom instructors to regulate the use of electronic devices
- Acknowledgement that administrators and technology staff may search a student's device memory when reasonable suspicion exists that a State or Federal law, CCID policy, or school rule has been violated
- Acknowledgement that administrators and technology staff 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
- Acknowledgement that violation of law will result in referral to law enforcement for possible criminal prosecution as well as disciplinary action by CCID

II. Use of Data Capture Devices By Students.

Students may use audio recording devices, cameras, video recording devices, messaging devices, or any device with data capture or communication capabilities except under the following conditions or circumstances:

- Direction not to use such devices by administration, law enforcement, a staff member, or those who are being recorded or about whom information is being shared
- In the event that audio and video recordings, photographs, or electronic communications violate reasonable expectations of privacy, current law, or CCID policy
- When audio and video recordings, photographs, or electronic communications include bullying, harassment, or intimidation, or cause interference with school operations or disruption of school activities

III. Student Access to Network.

Access to CCID's wireless network, including the internet, is permitted primarily for instructional purposes and is a privilege rather than a right. Limited personal use of CCID's network is permitted if the use meets the following conditions:

- Imposes no tangible cost to CCID
- Does not unduly burden or cause damage to CCID's computer or network resources

- Has no adverse effect on a student's academic performance

IV. Privately Owned, Student Devices

Students have the privilege of using privately owned electronic devices in compliance with State and Federal law, CCID policies, and school and classroom rules with the following acknowledgements:

- The right of administrators and technology staff to confiscate a privately owned device if Federal or State law, CCID policy, or school or classroom rules are violated
- The right of administrators and technology staff to search a privately owned device, when the use of the device most likely involved the school's network and/or resources to violate the law

In the event that a confiscated device is privately owned and CCID's network or 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.

V. Use of Devices by CCID Employees

Employees of CCID have the privilege of using electronic devices on CCID property or during CCID-sponsored activities pending the following:

- Receipt, understanding, and willingness to adhere to this policy and the *Employee Responsible Use Agreement*
- Receipt, understanding, and willingness to adhere to the rules and procedures developed at CCID that regulate the use of privately owned and CCID-owned devices
- Acknowledgement that administrators and technology staff may search an employee's device memory when reasonable suspicion exists that a State or federal law, CCID policy, or school rule has been violated
- Acknowledgement that administrators 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.

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

VI. Use of Data Capture Devices by CCID Employees

Employees may use audio recording devices, cameras, video recording devices, messaging devices, or any device with data capture or communication capabilities except under the following conditions or circumstances:

- Reasonable direction not to use such devices by administration, law enforcement, a staff member, or those who are being recorded or about whom information is being shared
- In the event that audio and video recordings, photographs, or electronic communications violate reasonable expectations of privacy, current law, or CCID policy

- When audio and video recordings, photographs, or electronic communications include bullying, harassment, or intimidation, or cause interference with school operations or disruption of school activities

VII. Employee Access to Network.

Access to CCID's wireless network, including the internet, is permitted primarily for instructional purposes and is a privilege rather than a right. Limited personal use of CCID's network is permitted if the use meets the following conditions:

- Imposes no tangible cost to CCID
- Does not unduly burden or cause damage to CCID's computer or network resources
- Has no adverse effect on an employee's job performance

VIII. Privately Owned, Employee Devices

Employees have the privilege of using privately owned electronic devices in compliance with State and Federal law, CCID policies, and school norms established by the administration with the following acknowledgement:

- The administration and technology staff will involve law enforcement to confiscate and search the privately owned device of a staff member when use of the device most likely involved violation of State or Federal law.

IX. Guest Use of Privately Owned Devices

Community members or guests may have the privilege of using privately owned electronic devices as described below:

- Community members or guests may use audio recording devices, cameras, video recording devices, messaging devices, or any device with data capture or communication capabilities while on school property or when officially accompanying students to a school-sponsored event, unless otherwise reasonably directed by the administration, law enforcement, a staff member, or those who are being recorded or about whom information is being shared
- Community members or guests 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 CCID policy
- Community members or guests may share audio, images, video, or any form of electronic communication with the exception of audio and video recordings, photographs, or electronic communications that bully, harass, intimidate, or cause interference with school operations or disrupt school activities

Violations of law will result in referral to law enforcement for possible criminal prosecution.

X. Wireless Guest Network

Community members or guests may have limited use of the CCID wireless guest network under the following conditions:

- Receipt, understanding, and willingness to adhere to this policy and, in particular, those aspects of this policy that govern community member and guest use
- That community member or guest use imposes no tangible cost to CCID
- That community member or guest use does not unduly burden or cause damage to CCID's computer or network resources

X. Reasonable Expectation to Record or Share

Examples of a reasonable expectation to record or share audio, video, or other forms of electronic communication include: a school assembly or special class presentation, sporting events, fairs or events where demonstrations take place, and locations where public activity is generally recorded or documented by the school.

XI. Procedures.

- Use agreements are signed annually or as soon as reasonably possible after the beginning of the school year
- Use agreements are stored by the administration where they may be verified by the administration or law enforcement as needed

XII. Enforcement

- When a student violates this policy, his/her electronic device may be confiscated.
- When an employee confiscates a student's device under this policy, he/she shall take reasonable measures to label and secure the device and then turn the device directly over to a school administrator or a staff member designated by the administrator for such a purpose, as soon as the employee's duties permit.
- A student's 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.

XIII. Investigations

- School administrators, in consultation with technology staff, 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 CCID's network for activities suspected of violating this policy.
- CCID's administrators and/or law enforcement may search CCID-created accounts and applications, as well as private accounts or applications accessed through the school's network for activities suspected of violating this policy.
- Privately owned devices, private accounts, or private applications used on CCID's property or at school-sponsored events suspected of violating State or Federal law will

be referred to law enforcement for investigation when CCID's network was clearly not involved in the use of the device, account, or application.
- CCID reserves the right to investigate the use history, downloads, or drives for any device accessing CCID's network, even when the use history, downloads, or drive configurations occurred on a network not provided by CCID.

XIV. Disciplinary Actions

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

- Suspension in or out of school
- Expulsion from school
- 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 an instructor
- Confiscation of device for increasing periods of time for repeat violations
- Other disciplinary actions as deemed appropriate by the CCID's Administration

XV. CCID Network Access

Employees, students, and guests shall do by the following in accessing CCID's network:

- Abide by all State and Federal law
- Use the internet primarily for education and instruction
- Conduct themselves in s responsible, decent, ethical, and polite manner
- Accept responsibility for adhering to high standards of personal, digital citizenship to ensure quality network access for all users expected in a school environment
- CCID provided devices and privately owned devices accessing CCID's network or its resources may be required to allow device management as specified by CCID's Administration

CCID is not responsible for the ability of privately owned devices to access CCID's network.

XVI. Authentication

- Personal and device information may be required when accessing CCID's network
- Information may include, but is not limited to: name, email, identifications, passwords, phone numbers, device credentials, etc.
- Network authentication processes are configured to support secure and safe data exchanges with CCID-owned devices for educational purposes

XVII. Filtering

All devices accessing CCID's network on or off CCID's 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).

CCID claims no liability for filtering related to the use of privately owned devices or CCID-provided devices on home networks or other networks not provided by CCID, 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 CCID.

XVIII. File Storage and Access

- CCID provides access to electronic storage for educational purposes, including, but not limited to: all supported electronic media, electronic curriculum, resources, etc.
- CCID's storage resources are available for secure access and protection of student and employee educational work and records.
- CCID's 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 backup, recovery systems, etc.

XIX. Power

- Those using devices on campus are expected to make reasonable preparations to power their devices before coming to campus for educational, instructional, or other school or district-sponsored activities.
- Students, employees, or guests may access power freely on CCID power sources unless otherwise directed by administrators or their designated representatives.

XX. Training

- All employees will be trained in current policy related to the use of technology in the classroom and at school activities annual and as soon as reasonably possible after a change in State or Federal law or CCID policy.
- All employees will be trained in the appropriate preservation and archiving of digital data
- Students will be trained yearly in Internet Safety in compliance with CIPA and will receive specific training in each of their individual classes on the appropriate use of electronic devices for those classes.

XXI. Liability

- 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 of the device.
- CCID takes no responsibility for stolen, lost, or damaged devices, including lost or corrupted data on those devices.

- CCID's students and employees, as 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 of CCID responsibly handling a privately owned device or a device assigned to another user, during the course of his/her duties, shall not be responsible for stolen, lost, or damaged devices, including lost or corrupted data on those devices.
- CCID employees and students are responsible for the replacement or repair of assigned devices that are lost, damaged, stolen while under their care.
- CCID and its employees are not responsible for device charges to private credit, online, or other accounts that might be incurred during approved school related use.
- CCID and its employees are not responsible for any device charges resulting from non-school related use of a device.
- CCID 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 CCID
    - Cyber theft from a privately owned device while on school district property
    - Cyber theft while participating in a CCID-sponsored activity
    - Cyber theft while using the school's network
    - Cyber theft while using a private network