WEILENMANN SCHOOL OF DISCOVERY
Responsible Technology Use Policy

Purpose
The Board of Directors of the Weilenmann School of Discovery ("WSD") recognizes the value of technologies to enhance and expand the learning process beyond the confines of the classroom and their potential to prepare students for 21st-century and post-secondary pathways. Although committed to providing students with access to technology devices, applications, Internet, and data systems for educational purposes, the board understands its legal obligation to protect students from harmful content on the Internet and to protect students' personal data from inappropriate dissemination.

In accordance with Utah State Code §53G-7-1002 and Utah Code §53G-7-1003, the policy ensures that parents, students, teachers, staff, and board members understand the rules and procedures that must be followed in order to access and use the school's Internet and electronic resources, and to use school-provided devices wherever these devices are used. The policy asserts that use of the school's network resources is a privilege that may be revoked at any time by the school's Administration for failure to comply with this policy or its administrative procedures described within this policy. The board delegates responsibility for implementing this policy to WSD's Administration.

Process and Content Standards
In according with Utah State Code §53G-7-1003, the school affirms that it restricts access to Internet or online sites that contain obscene material, that the school has adopted procedures and guidelines for staff to enforce this policy which are available for review at the school, and that procedures for receiving complaints about this policy, its enforcement, or observed behavior have also been adopted and are available for review at the school. This policy meets the requirements for a CIPA-compliant acceptable use policy as required by the FCC and satisfies the demands of annual certification through UETN.

Policy References
Relevant federal law, state law, and board rule that require, guide, and inform this policy include, but are not limited to, the following:

- Family Educational Rights and Privacy Act (FERPA)34 CFR, Part 99
- 47 CFR, Part 54, Children's Internet Protection Act (CIPA), which requires schools and libraries that have computers with internet access to certify they have internet safety policies and technology protection measures in place to receive discounted internet access and services.
- Utah State Code §53G-7-1002: Internet and Online Access Policy
- Utah State Code §53E-3-512 Employee Ethical Conduct Standards
- Utah State Board of Education R277-495: Electronic Devices in Public Schools

Definitions

- 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: a smart phone; a smart or electronic watch; a tablet; or a virtual reality 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, Chromebooks, and wearable technology; as well as portable storage devices such as hard drives, flash drives, SD Cards, and Microdrives.

- 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 teachers, staff, students, parents, board members, and guests.
- Guest means an individual: who is not a student, employee, or designated volunteer of the school, and who is on school property or at the site of a school-sponsored activity or event.
- Inappropriate Matter means pornographic or indecent material as defined in Utah Code Subsection 76-10-1253.
- Network means any wired or wireless system that allows for the exchange of data, including school networks, cellular networks, commercial, community, or home-based wireless networks accessible to students.
- Privately Owned Electronic Device means a device, including an electronic device that is used for audio, video, text communication, or another type of computer or computer-like instrument that is not owned or issued by the school to a student, employee, or guest.
- School-Owned Electronic Device means a device that is used for audio, video, text communication, or another type of computer or computer-like instrument that is identified as being owned, provided, issued or lent by the school to a student or employee.
- Student means an individual enrolled as a student at the school, regardless of the part-time nature of the enrollment or the age of the individual.
- Reasonable or Reasonably means efforts by administration, teachers, staff, or law enforcement to prevent disruption to instruction or other school sponsored activities, damage to school property, or interference with school operations within the confines of current state or federal law, school rules, or district policies.
- Responsible Technology Use Policy means WSD's policy delineating appropriate use of electronic devices, the Internet, or other electronic information resources while using a WSD device, WSD's connectivity, while at a school activity, on WSD's property, or anywhere using a school-owned device; also, the document stipulating constraints and practices that a user shall accept prior to using a school-owned device or accessing WSD's connectivity or Internet on or off school-owned property.
- The Children's Internet Protection Act (CIPA) means federal regulations enacted by the Federal Communications Commission (FCC) and administered by the Schools and Libraries Division of the FCC. CIPA and companion laws, the Neighborhood Children's Internet Protection Act (NCIPA) and the Protecting Children in the 21st Century Act, require recipients of federal technology funds to comply with certain Internet filtering and policy requirements.
- User means anyone, including teachers, staff, students, parents, board members, or guests, using a school-owned or privately owned electronic device, the school's connectivity or Internet, or any device or internet service while on school property or at a school activity.
- Utah Education Telehealth Network or UETN means the Utah Education and Telehealth Network created in Section 53B-17-105.

Prohibitions

In accordance with USBE R277-495-4, this policy expressly prohibits teachers, staff, board members, volunteers, students, parents, and guests from using a school-owned or privately owned electronic device, the school's connectivity or Internet, or any device or internet service while on school property or at a school activity, to engage in actions listed below:

- Violating local, state, or federal laws.
- Bullying, humiliating, harassing, or intimidating school-related individuals, including students, employees, and guests, consistent with USBE R277-609 and R277-613.
- Accessing inappropriate or obscene materials on the internet and world wide web while using the school's equipment, services, or connectivity, whether on or off school property.
- Compromising the safety and security of students when using social media and other forms of electronic communications.
- Engaging in unauthorized access, including hacking and other unlawful activities, while using the school's electronic device, services, or connectivity, whether on or off school property.
- Engaging in unauthorized disclosure, use, and/or dissemination of personal student information under USBE R277-487 and the Family Educational Rights and Privacy Act (FERPA)34 CFR, Part 99.
- Any use for illegal or inappropriate purposes or to access materials that are objectionable in a public school environment, or in support of such activities, is prohibited.
- Language that is deemed to be slanderous, libelous, vulgar, or pornographic is also prohibited.
- Illegal activities shall be defined as a violation of local, state, and/or federal laws.
- Inappropriate use shall be defined as a violation of the intended use of the network and could be subject to disciplinary action including criminal prosecution.
- This policy further prohibits accessing, transmitting, or retransmitting material that:
    - Promotes violence or advocates destruction of property including, but not limited to, access to information concerning the manufacture of destructive devices such as explosives, fireworks, smoke bombs, incendiary devices, or the like.
    - Contains pornographic or other sexually oriented material (such as pictures or writing that are intended to stimulate erotic feelings by the description or portrayal of sexual activity or nudity).
    - Advocates or promotes violence or hatred against particular individuals or groups of individuals, or advocates or promotes the superiority of one racial, ethnic, or religious group over another.

Procedures

Authority

- The school has the authority, and in some cases, the legal obligation to place restrictions on students' use of and access to electronic devices and school-provided computer systems, computer networks, school-adapted tools and devices, software applications, email, and the Internet ("electronic resources").
- The school has the authority to hold all students accountable for the ethical and legal utilization of the school's electronic resources when using these resources either on or off school property or at school activities. Students must comply with this policy as well as the board's Discipline Policy and its administrative procedures.
- The school has the authority at all times to revoke the privilege of students, teachers, staff, parents, or guests to access the school's electronic resources. Inappropriate use of electronic resources may result in a loss of network privileges, disciplinary action, and/or referral to legal authorities.
- The system administrator has the authority to close an account at any time.
- Additionally, an administrator has the authority to request that the system administrator deny, revoke or suspend an individual's access and/or account temporarily during an

investigation, and such a revocation will stand if an investigation yields sufficient evidence or concern to warrant it.
- Parents have the right at any time to terminate their child's access to the school's electronic resources by providing a written to the Administration asking for their child's access to be terminated.

Access to Electronic Resources
Parents, students, and employees, board members, and volunteers will attest that they have read, understand, and agree to abide by this policy and these administrative procedures through signing an "Electronic Device User Agreement" prior to accessing the school's electronic resources. In addition, the use of the school's electronic resources by any individual constitutes an implicit agreement to abide by this Responsible Technology Use Policy.

Training
In accordance with USBE R277-495-5, WSD provides the following training to students, teachers, and staff within the first 45 days of each school year:

- A schoolwide or in-classroom training that covers the contents of the school's Responsible Technology Use Policy and the administrative rules governing the use of technology in the classroom and at school activities.
- The importance of digital citizenship.
- The school's conduct and discipline-related consequences for violations of this policy.
- The school's general conduct and discipline policies as described in Section 53G-8-202.
- The benefits of connecting to the Internet and utilizing the school's internet filters while on school premises.
- Specific rules governing the permissible and restricted uses of personal electronic devices while in a classroom.
- The requirement that each educator who allows the use of a personal electronic device in the classroom clearly communicates to parents and students the conditions under which the use of a personal electronic device is allowed.
- Training for employees in the appropriate preservation and archiving of digital data.
- Training for students annually in Internet Safety in compliance with CIPA and on the appropriate use of electronic devices.

Required Notifications
The school will provide an annual notice to all parents of the location of information for in-home network filtering options as provided for in Section 76-10-1231.

Acceptable Use of Technology and Electronic Resources
Students
- Students must only use approved technology, services, and devices.
- A student's use of the school's electronic resources shall be for educational purposes only, which includes accessing and sharing information with teachers and other students, storing files, conducting research, and collaborating on projects.
- In some instances, students may be directed by their teachers to use the school's electronic resources in conjunction with their curriculum, an assessment, or an academic or behavior support program.
- Each student has access to a school device and accounts, and all communication between teachers, staff, and students should be performed using school accounts or devices.

- Students and their parents are responsible for costs associated with repairing damaged devices. If a student or parent is unable to pay for repairs, alternative forms of restitution may be established with the Administration.

Employees

- Employees must only use approved technology, services, and devices.
- All school-owned devices are on loan to employees for use in their essential job functions.
- Employees must secure the physical environment around their workspace and lock their computers when stepping away.
- Employees must ensure that Personally Identifiable Information (PII), confidential, and any sensitive data that may be covered by state or federal law, or board rule, is not readily available or accessible on their desks or within their workspace.
- All employees must take appropriate care to protect information, systems, and related assets within their custody or care from loss, damage, or harm.
- Employees must report lost or damaged equipment to the Administration as soon as practical.
- Employees are responsible for costs associated with repairing damaged devices.
- Employees must store their passwords in a secure manner.
- Employee-assigned accounts must only access assets, operating systems, applications, files, and data to which they have been granted access. The ability to inadvertently read, execute, modify, delete, or copy data does not imply permission to do so.
- Only authorized employees are permitted to post content or create the impression that they are representing, stating opinions, or otherwise making statements on behalf of the enterprise on social networking sites, blogs, or other Internet sites.
- Employees must keep confidential any knowledge about information and information systems gained during employment, and confidentiality must be maintained after employment ceases.
- Upon separation from the school, employees must return all supplied devices, assets, and the associated data.

Prohibited Uses of Technology for Employees

- Only approved and authorized devices may be connected to networks owned or managed by the school. This rule governs portable end-user devices, removable devices (e.g., USB sticks and privately owned devices).
- Users must not share their passwords with others or allow the use of their account by others. Users are responsible for all activity originating from their usernames and accounts.
- Users must not circumvent user authentication mechanisms or the security of any user account or information system asset.
- Users must not install software, hardware, or modify system configuration settings on any enterprise asset, unless explicitly permitted by the user's role and responsibility.
- Users must not engage in any activity with the intent to disrupt the school's assets or networks.
- Users must not perform any form of network monitoring, port scanning or security scanning unless the activity is part of the user's assigned work and has been formally authorized.
- Users must not leverage the school's assets for personal economic gain.
- Users must not leverage the "Remember" my password function inside of a browser.
- While users are permitted limited personal use of the school's assets, such as visiting websites, users may not use the school's assets for broad personal use of any kind,

including but not limited to, personal data storage, personal businesses, personal clubs, personal tutoring, personal official records, personal pictures and records, volunteer efforts, community organizations, social media, etc.
- School-sanctioned clubs or after-school activities run by WSD teachers for WSD students are permitted to use school devices, programs, applications, and accounts in order to support the activities whether teachers are paid by the school or directly by parents for their additional time and effort.
- Users must not use personally owned accounts (e.g., Apple ID, Google Account, Microsoft Account) for device-wide (e.g., Android, iOS, Windows) on school-owned devices.
- Users must not use school license keys on privately owned devices unless authorized by the school.
- School data must not be stored on non-school, personal cloud provider platforms (e.g., Google Drive, Microsoft OneDrive, Dropbox).

Prohibited Uses of Technology for All Users
- Any use that violates or supports the violation of federal, state, or local laws, board policy, school rules, and/or the student code of conduct, including any form of bullying, humiliation, intimidation, and harassment.
- Use of copyrighted materials or materials protected by trade secrets without appropriate authorization.
- Any use in violation of software license agreements.
- Any use that constitutes plagiarism.
- Vandalism and/or theft.
- Any deliberate attempt to damage the hardware, software, or information resident on the school's network or any other computer system attached through the Internet.
- Violating or attempting to violate the integrity of private accounts, files, or programs.
- Deliberately infecting a computer with a virus.
- Hacking computers using any method.
- Interfering with computer or network performance.
- Interfering with another's ability to use equipment and systems.
- Destroying data.
- Any use for commercial purposes or activities resulting in personal financial gain, including product advertisements and solicitations.
- Offensive or harassing behavior.
- Any use of material, whether visual or textual, that may be deemed profane, vulgar, pornographic, indecent, abusive, threatening, obscene, or sexually explicit.
- Distribution of disparaging or harassing statements including those that might incite violence of that are based on race, color, pregnancy, gender identity, genetic information, national origin, sex, sexual orientation, age, disability, or political or religious beliefs.
- Posting of anonymous messages.
- Any use for a religious or political purpose, including religious proselytizing and lobbying for student body elections.
- Using an account other than the student's assigned account.
- Accessing or attempting to access accounts, sites, servers, files, databases, or other systems for which a student is not authorized (such as hacking or using spyware).
- Spreading computer viruses.
- Degrading or disrupting network equipment, software, or system performance.
- Running applications or files that create a security risk.
- Any other action that threatens the security of the school's electronic resources.
- Transmitting confidential information about other individuals.

- Violating the privacy of others by reading or posting email or other private communications without obtaining the appropriate consent.
- Providing personal addresses, phone numbers, or financial information in any network communication whether that information belongs to the student user or any other individual unless it is related to an appropriate educational objective in the curriculum.
- Downloading or streaming audio or video files, or any other files that are not directly related to course curriculum.
- Playing non-educational Internet games.
- Accessing or using services on the Internet that impose a fee on a student.
- Any attempt to bypass state or school security.
- Attempting to disable or bypass the school's Internet blocking/filtering software without authorization.
- Adding, modifying, repairing, removing, reconfiguring, or tampering with any device on the school's network infrastructure.

Privacy
Teachers, staff, and students should have no expectation of privacy as to their communications on or use of the school's Internet or electronic resources. The school reserves the right to monitor whatever a user does on the school's network. In addition, Internet sites maintain records that can be subpoenaed to identify what the user has been viewing and downloading on the internet.

Security
WSD considers security as one of its highest priorities related to responsible technology use. If a security problem is identified, users should notify the Administration immediately. A security breach should *not* be demonstrated to others, nor should users demonstrate how to gain unauthorized access to sites, servers, files, etc. Users should *not* share passwords with other users but should change passwords frequently. Users should not leave an electronic workstation without logging out of the network.

Users must report to an Administrator when they receive or obtain information to which they are not entitled, when they know of any inappropriate use of the network by others, and when they believe the filtering software is not filtering a site or sites that should be filtered under this policy.

File Storage and Access
- WSD provides access to electronic storage for educational purposes, including, but not limited to all supported electronic media, electronic curriculum, electronic educational resources, etc.
- WSD's storage resources are available for secure access and protection of student and employee personally identifiable information, educational work, and records.
- WSD'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.

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

- In accordance with CIPA, the school utilizes and consistently configures filtering/blocking software to block access to sites and materials that are inappropriate, offensive, obscene, contain pornography, or are otherwise harmful to students.
- The school utilizes its best efforts to block access to such sites and materials but cannot guarantee the complete effectiveness of its filtering/blocking software.
- WSD claims no liability for filtering related to the use of privately owned devices or WSD-provided devices on home networks or other networks not provided by WSD, 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 WSD.

Limitations

Filtering Limitations

In accordance with state and federal law, WSD utilizes available technology protection measures to restrict students' access to Internet or online sites that contain obscene or inappropriate materials. However, the school acknowledges that, on a global network and with current protection measures, it is impossible to control all materials which a determined student may discover, including inappropriate information.

Therefore, in addition to its strict protection measures, the school requires all students to use the school's network resources in a responsible, ethical, courteous, efficient, and legal manner. To that end, teachers instruct and supervise students on the responsible use of Internet resources, proper network etiquette, and digital citizenship. Each student and the student's parent must sign an "Electronic Device User Agreement" at registration and/or annually.

Other Limitations

Other limitations include the following:

- WSD makes no warranties of any kind, whether expressed or implied, for the services it is providing. Electronic resources are provided on an "as is, as available," basis.
- The school will not be responsible for any damages a student may suffer while using its electronic resources which may include but are not limited to, loss of data resulting from delays, non-deliveries, or service interruptions caused by the system or by an individual's negligence, error, or omission.
- The school makes no promise or warranty to maintain or update its network, or the information contained therein.
- The school may suspend or discontinue these services at any time.
- Use of any information obtained via the information system is at the student's own risk.
- The school specifically denies any responsibility for the accuracy or appropriateness of information obtained through electronic resources.

Conditions of Use

General Terms of Use

Teachers, staff, and students have the privilege of using electronic devices and accessing electronic resources at or through the school pending acceptance of the following terms:

- Receiving, acknowledging, and signing an "Electronic Device User Agreement" annually or as soon as reasonably possible, such as at registration or shortly after the beginning of the school year.
- Understanding that "Electronic Device User Agreements" are stored by the Administration where they may be verified by the Administration or law enforcement as needed.

- Adhering to rules and procedures of the school and of individual classroom instructors concerning the use of electronic devices and access to electronic resources.
- Acknowledgement that administrators, teachers, and staff may search a student's device memory when reasonable suspicion exists that a State or Federal law, a WSD policy, or a school rule has been violated.
- Acknowledgement that administrators, teachers, and 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 WSD.

WSD Network Access

Employees, teachers, staff, students, and guests shall abide by the following guidelines in accessing WSD's network and electronic resources:

- Abide by all state and federal law.
- Use the Internet primarily for education and instruction.
- Conduct themselves in a responsible, decent, ethical, and polite manner.
- Accept responsibility for adhering to the high standards of personal, digital citizenship expected in a school environment.
- Consent to the device management required or specified by WSD's Director of Technology, including for privately owned devices accessing WSD's network or its electronic resources.

Authentication

- Personal and device information may be required when accessing WSD's network and electronic resources.
- 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 school-owned devices for educational purposes.

Power for Devices

- 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 WSD power sources unless otherwise directed by Administrators or their designated representatives.

Liability Related to Electronic 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 of the device.
- WSD takes no responsibility for stolen, lost, or damaged devices, including lost or corrupted data on those devices.
- WSD'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 WSD handling a privately owned device or a device assigned to another user reasonably 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.

- WSD employees and students are responsible for the replacement or repair of assigned devices that are lost, damaged, or stolen while under their care.
- WSD 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.
- WSD and its employees are not responsible for any device charges resulting from non-school related use of a device.
- WSD 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 WSD.
    - Cyber theft from a privately owned device while on school district property.
    - Cyber theft while participating in a WSD-sponsored activity.
    - Cyber theft while using the school's network.
    - Cyber theft while using a private network.

Student Access to Network

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

- Imposes no tangible cost to the school.
- Does not unduly burden or cause damage to the school's computer or network resources.
- Has no adverse effect on a student's academic performance.

Privately Owned Student Devices

Students may only use school-owned devices in the classroom. However, students may use privately owned electronic devices at designated times in compliance with state and federal law, WSD policies, and school rules with the following acknowledgements:

- The right of Administrators, teachers, and staff to confiscate a privately owned device if state or federal law, WSD policy, or school or classroom rules have been violated.
- The right of Administrators, teachers, and 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.
- The right of Administrators to turn over a privately owned device to law enforcement for initial or subsequent investigation(s) when a confiscated device has been involved in suspicious activity related to state or federal law, and even when WSD's network or resources were likely not involved.

Use of Data Capture Devices By Students

Students may only use school-owned devices for data capture including audio recordings, video recordings, messaging, or other data for educational purposes. Students may not use school-owned devices for data capture, including audio recordings, video records, messaging, or other data under the following conditions or circumstances:

- Direction not to use such devices by Administration, teachers, staff, law enforcement, 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, state or federal law, or school 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.

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

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

Privately Owned Employee Devices
WSD employees have the privilege of using privately owned and school-owned electronic devices on WSD's property and at school activities in compliance with state and federal law with the following acknowledgements:

- Receipt, understanding, and willingness to adhere to this policy
- Signing and adhering to the terms of the "Electronic Device User Agreement."
- Acknowledgement that privately owned devices must not be connected to the school network without formal authorization.
- Acknowledgement that school data must not be stored on privately owned devices without formal authorization.
- Receipt, understanding, and willingness to adhere to WSD's rules and procedures governing employee use of devices and access to electronic resources at WSD that regulate the use of privately owned and school-owned devices.
- Acknowledgement that administrators and technology staff may search an employee's school-owned device memory when reasonable suspicion exists that state or federal law, a WSD policy, or a 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, a report of the infraction of professional ethical standards to Utah Professional Practices Advisory Commission ("UPPAC"), and potential disciplinary action by WSD.
- Acknowledgement that users leveraging their privately owned devices to store school data may have their devices completely wiped. Reasons for device wipe may include:
    - Lost/stolen device.
    - Termination of user's employment.
    - Compromised/hacked account or device.

Use of Data Capture Devices by WSD Employees
Employees may only capture audio recordings, video recordings, messaging, or any other data on campus or at school activities with a school-owned device with the following limitations:

- 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, state or federal law, or WSD 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.

Wireless Guest Network

Community members or guests may have limited use of the WSD 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 specifically govern guests' use of devices and access to the school's electronic resources.
- That community member or guest use imposes no tangible cost to WSD.
- That community member or guest use does not unduly burden or cause damage to WSD's computers, network, or electronic resources.

Guest Use of Privately Owned Devices

Community members or guests have the privilege of using privately owned electronic devices to access WSD's Internet or electronic resources 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, teachers, staff, law enforcement, or those who are being recorded or about whom information is being shared.
- Community members or guests may not 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, state or federal law, or WSD policy.
- Community members or guests may not 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.
- In all instances, guests must be guided in sharing of any audio, images, video, or any form of electronic communication by administrators, teachers, and staff who are aware of families who have opted their students out of the sharing of such information with the exception of Directory Information.
- A reasonable expectation to record and share electronic information may include audio, images, or video from 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.
- Violations of law will result in referral to law enforcement for possible criminal prosecution.

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, the employee will take reasonable measures to label and secure the device and then turn the device 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.
- Based on a student's behavior related to the "Electronic Device User Agreement," the Administration may determine to take a student's device for *a* specific period of time or to revoke a student's privileges to use any device or access any electronic resources for the remainder of the school year.

Investigations

- In accordance with state and federal law, Administrators will determine whether to investigate and/or make a referral to law enforcement for investigation concerning the use of electronic devices and access of electronic resources at WSD in accordance with state and federal law.
- Administrators and/or law enforcement may search school district issued devices as well as privately owned devices that have used WSD's network for activities suspected of violating this policy or state or federal law.
- Administrators and/or law enforcement may search WSD-created accounts and applications, as well as private accounts or applications accessed through the school's network, for activities suspected of violating this policy and state or federal law.
- Privately owned devices, private accounts, or private applications used on WSD's property or at school events that are suspected of having violated state or federal law will be referred to law enforcement for investigation even when WSD's network was not involved in the use of the device, account, or application.
- WSD reserves the right to investigate the use history, downloads, or drives for any school-owned device or device used on campus or at a school event, even when the use history, downloads, or drive configurations occurred on a network not provided by WSD.

Discipline and Termination of Accounts

Authorized school employees will be responsible to determine what constitutes a violation of this policy and its procedures. Authorized school employees have the right to intercept or read a student's email, review any material, edit or remove any material which they believe may be unlawful, obscene, defamatory, abusive, or otherwise objectionable.

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

- An in-school or out-of-school suspension.
- Expulsion from school.
- Notification of law enforcement authorities.
- Permanent prohibition from possession of an electronic device at school or school-related events.
- Supervised, temporary access to an electronic device for instruction as deemed necessary by an instructor.
- Confiscation of a device for increasing periods of time for repeat violations.
- Other disciplinary actions as deemed appropriate by the Administration.
- If the school intends to impose any discipline, other than revoking privileges for the remainder of the school year, the student will be afforded due process.
- An account will be terminated under the following circumstances:
    - The student's parent makes a request in writing to an Administrator that the account be terminated.
    - Any authorized Administrator determines the account should be terminated.
    - A student's family withdraws the student from the school.

Approved: September 26, 2023