

Acceptable Use Policy_Staff | Version 1.2

Policy

Internal Use Only

Effective: July 1, 2024

Approved By: Bob Fishtrom

Reviewed Date: July 1, 2024

Table of Contents

1.0 Introduction 3

1.1 Purpose 3

1.2 Ownership 4

1.3 Prohibited Uses 6

1.4 Equipment Loss 7

1.5 Social Networking 8

1.6 Free Speech 8

1.7 Intellectual Property 8

1.8 Limitations on District Responsibility 9

1.9 Appropriate Use of Student Information 9

Procedures Appendix 11

California Electronic Communications Privacy Act (CalECPA) 11

Equipment Loss Procedure 15

1.0 Introduction

This Staff Technology Acceptable Use Agreement (“AUP”) protects Mountain View–Los Altos School District (“**MVLA**”) and its employees by providing guidelines and regulations for the appropriate use of District technology, information, and communication.

By using District technology, employees agree to abide by all of the terms described in this AUP. This AUP applies when District technology is accessed on or off-site, both through District-owned or personally owned equipment or devices.

District technology includes, but is not limited to, District-owned and/or District managed computing devices and peripherals (e.g., computers, laptops, tablets, projection systems, printers, storage devices, wearable technology, etc.), District network and communication devices/services (telephones, wired and wireless networks including WiFi access points, emergency radios, email systems, file servers, etc.), and District managed on-line services/access to online information sources, and future technological innovations (such as Google Workspace, Aeries Student Information System, Office365, Adobe Creative Cloud, and other services).

1.1 Purpose

The purpose and considerations reflected in this MVLA Acceptable Use Policy (AUP) include, but are not limited to:

- Protecting the welfare of children;
- Protecting individuals’ right to privacy;
- Protecting intellectual and property rights;
- Respecting the rights of students, parents/guardians, and staff;
- Protecting District technology and electronic information;
- Assuring District resources are used to promote the District’s educational goals;
- Assuring District technology and other information resources are accessible to all, well designed, and easy to navigate; and

- Assuring all employees adhere to the highest standards of professionalism, integrity, and civility.
- The MVLA District provides a wide range of technology to its employees for the purpose of advancing the District's educational mission, which includes classroom instruction, information processing for school business, and enhancing communication between District employees, parents, students, and community members. The District's goal for using technology is to promote educational excellence in schools by providing appropriate access to all students; fully integrating technology into the daily curriculum; modeling and promoting digital citizenship; facilitating critical thinking, creativity, communication, and collaboration; and preparing students and educators to meet the challenge of participating in a dynamic global society.

All MVLA District employees are expected to learn and use the available technological resources that will assist them in the performance of their job responsibilities. Resources are provided at the public's expense and maintained by the District and are to be used by employees with respect for the public trust through which they have been provided. The District intends to maintain a nonpublic forum, and the forums created by use of District technology are reserved for the District's intended purposes.

The successful operation of District technology requires that all users conduct themselves in a responsible, confidential, ethical, professional, and polite manner, consistent with the District's mission and goals, as well as all applicable laws and regulations. This AUP does not attempt to articulate every single required or prohibited behavior by employees. The District Technology Department can provide additional guidance, support, or clarification when needed.

1.2 Ownership

Employees have no specific ownership or possessory right in District-owned devices used or in the information stored or created therein.

Upon receipt of a MVLA District-owned device, employees may be the authorized possessor as defined in the California Electronic Communications Privacy Act (CalECPA). As an authorized possessor of a District-owned device, employees are responsible for using the device appropriately and for employment-related purposes.

- Only the employee assigned by the District to the device may use the device.
- The District may confiscate any District-owned device at any time and without cause. If the District confiscates a District-owned device, an employee is no longer the authorized possessor of the device.
- District-owned devices are the property of the District. District-owned devices and the information contained therein may be assigned or used by other employees, on an as-needed basis, in furtherance of the District's operational and administrative objectives.
- Employees have no reasonable expectation of privacy in using District managed technology and services.
- An employee's use of District technology is a waiver of the protections of CalECPA. By using District technology, whether from personal or District-owned devices, employees grant specific consent, as defined by CalECPA, to the District to review and monitor all electronic communication information and electronic device information created, stored, or transmitted via District technology.
- The data that employees create, store, and/or transmit using District technology is not private and is considered the property of the District, even when employees use a password to secure the device or service.
- The District retains the right to inspect, delete, and report any apps, information, and files on District technology. Employees uncomfortable with this stipulation should refrain from loading personal information, files, apps, and email accounts onto District-owned devices.
- Employees are prohibited from bringing illegal content onto District technology. The District will comply with all legal requirements for notification and reporting of any illegal activity or suspected illegal activity to law enforcement officials.
- Employees who choose to access District technology services (e.g., the District's network) on their personal devices acknowledge and agree to turn over their personally owned devices and/or equipment when requested by law enforcement officials as a condition of accessing District technology services from those devices. Employees who do not agree to these stipulations must refrain from using their personally owned devices and equipment to access and communicate via District technology.

- Employees shall periodically examine their district electronic devices and purge them of any personal files, photos, and videos unrelated to the District's educational mission.
- All District employees are to conduct official business and correspondence only through District provided or District managed accounts and not through their personal accounts.
- District/school business communications are subject to discovery pursuant to a subpoena, public records act request, or other lawful requests.
- District employees who conduct official District/school communications from their own personal, non-district issued devices acknowledge and agree that, in doing so, those personal devices may be subject to discovery and disclosure pursuant to a subpoena, public records act request or other lawful requests.
- District and/or school records maintained on any personally owned device or official communications sent or received on a personally owned device may be subject to discovery and disclosure, pursuant to a subpoena, public records act request, or other lawful requests.
- District-provided email accounts are strictly for educational business use and shall not be used for personal purposes.
- Accounts used to access District technology services must be kept secure (e.g., device logins, email, file storage, student information systems, electronic grade books, attendance and grade reporting functions, etc.)
- Employees are required to keep their passwords secure and shall not write down their passwords anywhere near the computer or where a student or other unauthorized user might discover them.
- Under no circumstances are employees to give their password(s) to students or let students or other unauthorized users input grades or attendance information into grade book/attendance programs.

Procedure: [California Electronic Communications Privacy Act \(CalECPA\)](#) (See Appendix)

1.3 Prohibited Uses

The following non-exhaustive list is intended to provide employees with examples of prohibited conduct, but is not intended to serve as a comprehensive list of potential employee misconduct related to the impermissible use of MVLA District technology:

- Creation and transmission of material that a recipient might consider disparaging, harassing, and/or abusive based on race, ethnicity, national origin, immigration status, sex, gender, sexual orientation, age, disability, religion, and/or political beliefs.
- Accessing, creating, publishing, or transmitting harmful or inappropriate matter that is sexually explicit, obscene, or threatening or that promotes any activity prohibited by law, Board policy, or administrative regulation;
- Creating, transmitting, or publishing defamatory material;
- Engaging in plagiarism;
- Infringing upon copyright, including software, published texts, and student work, or storing and/or public showing of audio and video media for which proper license or ownership is not maintained;
- Transmission of commercial and/or advertising material;
- Political and/or religious proselytizing;
- Intentionally interfering with the normal operation of District technology, including the willful propagation of computer viruses, use of spyware, or other malware;
- Causing congestion or disruption to District technology through inappropriate downloads of large files, streaming audio/video not directly related to providing instruction or district business, or other such non-work-related activities;
- Accessing, changing, or using another person's account, files, output, records, or username for which one does not have explicit authorization to do so.

1.4 Equipment Loss

In the event of damage or loss of MVLA District technology equipment, employees shall complete the District "Tech Equipment Loss Report Form" as soon as possible and submit it to the District Technology Department.

If a District device is stolen from an employee, he/she must obtain a police report and attach it to the Loss Report Form.

This may allow the District to seek reimbursement from its own insurance carrier in certain cases, among other reasons.

Procedure: [Equipment Loss Procedure](#) (See Appendix)

1.5 Social Networking

Employees may use social networking tools for appropriate educational purposes but should only use accounts created specifically for class communication and not personal account.

- Such purposes may include clubs, athletic teams, and co-curricular activities.

1.6 Free Speech

An MVLA District employee acting in an individual capacity and outside the scope of employment may, during non-working time, express views and opinions that do not necessarily state or reflect those of the District.

- Any such expression shall neither state nor imply that it is made on behalf of the District.
- A District employee shall not communicate information otherwise prohibited by District policy and procedures using District technology.

1.7 Intellectual Property

The MVLA District recognizes that employees may create instructional materials or online resources in the course of their employment in carrying out their duties as educators. The District shall retain a non-exclusive perpetual license in perpetuity to use, modify, and adapt the materials and resources created while under employment by the District for the purpose of carrying out the staff member's duties. The materials and resources otherwise remain the property of the author who is free to take the material with them when they leave the District.

Misuse of technology may result in discipline, penalties under applicable laws, and/or the loss of technology. Users may be held accountable for their conduct under any applicable District policy or collective bargaining agreement.

Illegal production or distribution of software and other intellectual property protected by U.S. copyright law is subject to civil damages and criminal punishment including fines and imprisonment.

1.8 Limitations on District Responsibility

The District makes no guarantee that the functions or services provided by or through District Technology will be without defect or uninterrupted. The District is not responsible for any damages suffered while utilizing District Technology.

The District is not responsible for any loss or damage incurred by an employee as a result of his/her personal use of District Technology.

The District is not responsible for any financial obligations arising from unauthorized use of District Technology.

1.9 Appropriate Use of Student Information

1. Student information can only be housed on district-owned devices and transmitted using district-approved communication channels and platforms.
 - a. The current platforms approved for use are district email, ParentSquare, Canvas LMS, and Aeries SIS. (updated 4/2024)
 - b. District-approved contractors shall be issued District owned and maintained devices as are all employees, in order to ensure appropriate storage and transmission of student information
2. Staff members must refrain from transmitting student information through personal email accounts, messaging apps, or other non-district-approved means.
 - a. When sending student information electronically, staff members must ensure encryption and secure transmission protocols are in place to safeguard data integrity and confidentiality.

- i. The platforms identified in item 1 (above) all send information using proper encryption and secure transmission protocols.

3. Artificial Intelligence (AI) and Student Information

- a. **With the emergence of artificial intelligence tools, staff members are only permitted to use district-approved AI platforms.**
 - i. **The currently approved platform for MVLA is Brisk Teaching**
- b. **When using such tools, staff members can not use students' personally identifiable information (names, student numbers, email addresses, etc.) when submitting information into the AI tool/generator.**

4. Compliance and Enforcement

- a. Failure to comply with this policy may result in disciplinary action
- b. Staff members violating this policy may be subject to legal consequences per relevant district, state, and federal regulations.

5. Training and Awareness

- a. All staff members shall receive training on properly handling and transmitting student information as part of their orientation and ongoing professional development.
- b. Periodic reminders and updates regarding this policy shall be communicated to staff members to ensure continued compliance.

6. Reporting

- a. Any suspected breaches or violations of this policy must be reported immediately to the designated district authorities for investigation and resolution.

7. Review and Revision

- a. This policy shall be reviewed annually and updated as necessary to reflect changes in technology, regulations, or organizational requirements.
- b. Amendments to this policy shall be communicated to all staff members in a timely manner.

Procedures Appendix

California Electronic Communications Privacy Act (CalECPA)

The California Electronic Communications Privacy Act (CalECPA), S.B. 178, requires state law enforcement to get a warrant before they can access electronic information about who we are, where we go, who we know, and what we do.

This bill creates the California Electronic Communications Privacy Act (CalECPA), which generally requires law enforcement entities to obtain a search warrant before accessing data on an electronic device or from an online service provider.

- Prohibits law enforcement from:
 - Compelling the production of or access to electronic communication information from a service provider.
 - Compelling the production of or access to electronic device information from any person or entity other than the authorized possessor of the device.
 - Accessing electronic device information by means of physical interaction or electronic communication with the device, although voluntary disclosure to a government entity is permitted.
- Permits a government entity to access electronic device information by means of physical interaction or electronic communication with the device only as follows:
 - Pursuant to a warrant;
 - Pursuant to a wiretap order;
 - With the specific consent of the authorized possessor of the device;
 - With the specific consent of the owner of the device, only when the device has been reported as lost or stolen;
 - If the government entity, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires access to the electronic device information;
 - If the government entity, in good faith, believes the device to be lost, stolen, or abandoned, provided that the entity shall only access electronic device

information in order to attempt to identify, verify, or contact the owner or authorized possessor of the device; and

- If the device is seized from an inmate's possession or found in an area of a correctional facility where inmates have access and the device is not in the possession of an individual and the device is not known or believed to be the possession of an authorized visitor, except as otherwise provided by state or federal law.
- Requires any warrant for electronic information to comply with the following:
 - The warrant shall describe with particularity the information to be seized, including by specifying the time periods covered, and as appropriate and reasonable, the target individuals or accounts, the applications or services covered, and the types of information sought;
 - The warrant shall require that any obtained information unrelated to the objective of the warrant shall be sealed and not subject to further review, use, or disclosure unless a court issues an order that there is probable cause to believe that the information is relevant to an active investigation, or is otherwise required by state or federal law; and
 - The warrant or order shall comply with all other provisions of California and federal law, including any provisions prohibiting, limiting, or imposing additional requirements on the use of search warrants. Warrants directed to a service provider must be accompanied by an order to verify the authenticity of the electronic information produced, as specified.
- When issuing any warrant for electronic information, or upon the petition from the target or recipient of the warrant, a court may, at its discretion, do any or all of the following:
 - Appoint a special master, who is charged with ensuring that only information necessary to achieve the objective of the warrant or order is produced or accessed.
 - Require that any information obtained through the execution of the warrant or order that is unrelated to the objective of the warrant be destroyed as soon as feasible after termination of current or related investigations.

- Authorizes a service provider to voluntarily disclose electronic communication information or subscriber information when that disclosure is not otherwise prohibited by state or federal law.
- Requires a government entity that receives electronic communication information voluntarily provided by a service provider to destroy that information within 90 days unless the entity has or obtains the specific consent of the sender or recipient, obtains a court order, or the information is retained for the investigation of child pornography and related crimes, as specified.
- Requires a government entity that obtains electronic information pursuant to an emergency to seek an authorizing warrant or order, or an approval motion, within three days after obtaining the electronic information, from the appropriate court, as specified.
- Declares that these provisions do not limit the authority of a government entity to use an administrative, grand jury, trial, or civil discovery subpoena to do either of the following:
 - Require an originator, addressee, or intended recipient of an electronic communication to disclose any electronic communication information associated with that communication;
 - Require an entity that provides electronic communications services to its officers, directors, employees, or agents for the purpose of carrying out their duties, to disclose electronic communication information associated with an electronic communication to or from an officer, director, employee, or agent of the entity; or,
 - Require a service provider to provide subscriber information.
- Requires a government entity that executes a warrant or obtains electronic information in an emergency pursuant to these provisions to serve or deliver a notice, as specified, to the identified targets stating that information about the target has been compelled or requested, and states with reasonable specificity the nature of the government investigation under which the information is sought, including a copy of the warrant, or a written statement setting forth facts giving rise to the emergency.

- Authorizes the government entity, when a search warrant is sought or electronic information obtained under emergency circumstances, to submit a request supported by a sworn affidavit for an order delaying notification and prohibiting any party providing information from notifying any other party that information has been sought. Further requires the court to issue the order if the court determines that there is reason to believe that notification may have an adverse result, not to exceed 90 days, and the court may grant extensions of the delay of up to 90 days each, as specified.
- Requires, upon expiration of the period of delay of the notification, the government entity to serve or deliver to the identified targets of the warrant a document that includes the information required in 10 above, as well as a copy of all electronic information obtained or a summary of that information, and a statement of the grounds for the court's determination to grant a delay in notifying the target, as specified.
- Provides that if there is no identified target of a warrant or emergency request at the time of issuance, the government entity shall submit to the DOJ within three days of the execution of the warrant or issuance of the request all of the information required in 10 above. If an order delaying notice is obtained, the government entity shall submit to DOJ upon the expiration of the period of delay of the notification the information required in 12 above. DOJ shall publish those reports on its web site within 90 days of receipt, and may redact names or other personal identifying information from the reports.
- Declares that nothing in these provisions shall prohibit or limit a service provider or any other party from disclosing information about any request or demand for electronic information, except as provided.
- Permits any person in a trial, hearing, or proceeding to move to suppress any electronic information obtained or retained in violation of the Fourth Amendment to the United States Constitution or of this chapter, as specified.
- Authorizes the Attorney General to commence a civil action to compel any government entity to comply with these provisions.
- Authorizes an individual whose information is targeted by a warrant, order, or other legal process that is inconsistent with these provisions, or the California Constitution or the United States Constitution, or a service provider or any other

recipient of the warrant, order, or other legal process, to petition the issuing court to void or modify the warrant, order, or process, or to order the destruction of any information obtained in violation of this chapter, the California Constitution, or the United States Constitution.

- Declares that a California or foreign corporation, and its officers, employees, and agents, are not subject to any cause of action for providing records, information, facilities, or assistance in accordance with the terms of a warrant, court order, statutory authorization, emergency certification, or wiretap order issued pursuant to these provisions.

Equipment Loss Procedure

In the event of damage or loss of District technology equipment,

- Employees shall complete the District “Tech Equipment Loss Report Form” as soon as possible and submit it to the District Technology Department.
- If a District device is stolen from an employee, he/she must obtain a police report and attach it to the Loss Report Form.
 - This may allow the District to seek reimbursement from its own insurance carrier in certain cases, among other reasons.