MVLA HIGH SCHOOL DISTRICT **MVLA**

Acceptable Use Policy_Staff | Version 1.1

Policy and Procedures

Internal Use Only

Effective: June 30, 2022

Table of Contents

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.

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.

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.