Using Technology in School
Acceptable Use Policy (AUP) for Students

The Conejo Valley Unified School District (CVUSD) has implemented the usage of the Measure I technology endowment fund to provide additional support for its 21st Century learners. Excellence in education requires that technology is seamlessly integrated throughout the instructional program. The individual or collaborative use of classroom student devices is one strategy to empower students to maximize their full potential and prepare them for college and career.

To this end, CVUSD provides secure computer and internet access to all students under its 1:1 Chromebook program. Student devices are to be used solely for educational purposes. This policy outlines appropriate use and prohibited activities. Each student is expected to follow the rules and conditions listed in this document and any directions or guidelines given by CVUSD teachers, substitutes, administrators, and staff.

All District Chromebooks, regardless of physical location (in and out of school), will have Internet activity protected and monitored by teachers, school administrators, and the technology staff. CVUSD uses an Internet content filter compliant with the federally mandated Children's Internet Protection Act (CIPA). CVUSD educators may request a specific website be evaluated to be blocked or unblocked by contacting the Technology Services Help Desk.

It is essential to understand that no filtering system is perfect. Due to the nature of the Internet and evolving technology, even with supervision and partnership with leading content vendors, the District cannot guarantee that students will not reach an inappropriate site. It is the student's responsibility to report any inappropriate sites to the teacher.

All activities conducted on the CVUSD network will be monitored by District administration to ensure compliance with the guidelines outlined in this document and local, state, and federal laws. There is no expectation of privacy with respect to the CVUSD network, and any activity, files, or messages transmitted on the network may be monitored at any time without notice. CVUSD may share such transmissions with the Student's Parent/Guardian and School staff. The consequences of improper use of the CVUSD network may result in disciplinary action, including removing all technology access.

Below are examples, but not an exhaustive list, of online conduct that may constitute a violation of federal and/or state criminal laws relating to cybercrimes:

- **Criminal Acts:** These include, but are not limited to, "hacking" or attempting to access computer systems without authorization, threatening/harassing via email, cyberstalking, various explicit content, vandalism, unauthorized tampering with computer systems, using misleading domain names, using another person's identity and/or identity fraud.
- **Libel Laws:** Publicly defaming people through publishing material on the Internet, email, etc.
- **Copyright Violations:** Copying, selling, or distributing copyrighted material without the express written permission of the author or publisher (users should assume that all materials available on the Internet are protected by copyright); engaging in plagiarism (using other's words or ideas as your own).

General Guidelines

The following protocols are provided to parents and students as a guideline of expectations only. Students will:

- Use all technology devices, peripherals, and resources in a responsible manner so as not to damage school and District equipment.
- Carry the device with two hands or like a book and make sure the lid or case cover is closed when transporting.
- Limit device exposure to direct sunlight.
- Never leave a device unattended, both in and out of the classroom.
- Keep the device away from water and other liquids, such as sprinklers, rain, puddles, and beverages.
- Not adhere stickers, ink, or other decorative items to school devices.
- Not allow others access to their District-owned devices and equipment
- Immediately report any lost or stolen devices

Student Behavior Guidelines and Digital Citizenship

Students are expected to exercise responsible academic behavior and Digital Citizenship when using the CVUSD network and technology equipment.

- General Use:
    - Report any problems with a school device, network, or other systems to the teacher.
    - Stay on task and follow the directions of CVUSD site and District staff.
    - Device sound is to be muted at all times during instruction unless otherwise directed by a teacher.
    - All devices are to be used only for academic purposes during instructional time. Students are not to access movies, games, or non-academic websites during class time unless granted permission by a teacher.
    - Do not attempt to bypass security settings or Internet filters or interfere with the operation of the network, including other devices connected to the network. Software designed to do so is prohibited on the CVUSD network. Such software includes but is not limited to file sharing, VPN tunnels, port scanners, DDOS, or malware software.
    - The installation of unauthorized software, including browser extensions, on school computers, is prohibited. Such software includes but is not limited to unapproved games and shareware.
    - It is important to log off the device at the end of every session so another user cannot use passwords that are not their own.
- Digital Citizenship:
    - Students are expected to keep their username and password private. Password information should not be shared with other students.
    - Students are expected to follow all copyright laws. If there is a question regarding copyright, please consult with the teacher.
    - Academic honesty is expected per CVUSD Board Policy and CVUSD Administrative Regulation 5131.9. Students are to complete their own work, referencing sources as required.
    - Students are responsible for their CVUSD account and are not to access another individual's account. Students are not to impersonate, spoof, or otherwise pretend to be someone else online. This includes, but is not limited to, sending out email, creating accounts, or posting messages or other online content (e.g. text, images, audio, or video) in someone else's name.

- Students are responsible for using appropriate language, both in class and online. This includes sending hateful or harassing email, making discriminatory remarks about others, and engaging in bullying, harassment, or other anti-social behaviors.
- Students are not to access another student's device without expressed permission.
- Anything done on social networking websites should not negatively impact the school learning environment and/or fellow students, teachers, and administrators.
- Students will not search, retrieve, save, circulate, or display hate-based, offensive, or sexually explicit material. Do not search, retrieve, save, or circulate images or information about weapons using any CVUSD computer resources unless authorized by school administrator/teacher as part of a school assignment.
- It is both unsafe and not recommended to post any personal information about oneself or others online, including but not limited to name, address, phone number, or school.
- Do not post photos of others with their first and last names on any online site, including but not limited to blogs, wikis, and discussions forums.

Classroom and Take-Home Devices: Logging In, Connecting to the Network, and Basic Troubleshooting

District-issued Chromebooks are enrolled under the **learn.conejousd.net** domain, making them inapplicable for any other use. In cases where a student is required to login to a device or system, each student is expected to utilize his/her individual, District-provided Google account (*example: 123456@learn.conejousd.net*) username and password to access equipment owned and maintained by CVUSD. Should a student forget his/her username or password, the student should ask one of his/her teachers to retrieve it.

District-owned devices are pre-configured to connect to the appropriate CVUSD Ethernet or WiFi network automatically. Should devices not automatically connect to the configured network, students should speak with the teacher regarding obtaining a temporary replacement device and/or further instructions.

CVUSD makes every reasonable effort to ensure classroom technology stays in proper working order. Nonetheless, the nature of modern technology lends itself to occasional downtime. The following basic troubleshooting tips are provided in the best supporting classroom instruction.

- If the device will NOT power on:
  - Ensure the device has been charged or is plugged into a power outlet.
- If the student is unable to login to the device:
  - Ensure the CAPS lock is not turned on.
  - Check the student's username and password combination to ensure that the appropriate one is being used.
  - Each student's teacher may print a copy of student passwords for Windows-based devices, Google Apps, and Q Student Connect via the Q Reports screen.
- Peripherals not functioning properly:
  - Is the peripheral plugged into the device?
  - Unplug the peripheral from the device, wait 10 seconds, plug the peripheral back into the device. o Plug the peripheral into a different port on the device (if available).
- Reboot the device.
- When all else fails please inform the teacher.

Classroom Technology Devices

Guidelines for Device Distribution and Return

Each CVUSD classroom teacher will, at his/her discretion, implement and communicate the device distribution and retrieval rules and expectations for the classroom.

Students will:

- Exercise care when removing and returning devices to the designated classroom storage cupboard.
- Exercise care when unplugging a device from its power cord.
- When returning a device, utilize the device's designated cupboard device slot and plug in the device's individual power cord.
- Return the device at the end of a class session or at the discretion of site and District staff members. If a student refuses to return a device, it may be reported stolen to the Thousand Oaks Police Department.
- Will not modify the hardware, security measures, or software loaded on the device.

Parent and Student Liability for Classroom Devices:

Students are expected to treat school and classroom devices with the appropriate care and respect. As applicable, the CVUSD student behavior policies will be enforced regarding any damage to school or classroom devices. Damage includes, but is not limited to, broken screens, cracked casing, inoperability, water damage, etc.

Student Take-Home Devices

Guidelines for Device Distribution and Return

Each CVUSD school site will, at its discretion, determine specific procedures and policies for distributing and retrieving 1:1 student take-home devices. The following guidelines are provided to schools, parents, and students as a guideline of expectations. Students will:

- Pick up and return the devices at the location designated by the school.
- Exercise care when picking up/returning a device.
- Return the device and any additional accessories such as a power cord by the specified deadline.

Parent and Student Liability for Take-Home Devices:

Take-home devices are for student use only. Students are expected to treat school and classroom devices with the appropriate care and respect. As applicable, the CVUSD student behavior policies will be enforced regarding any damage to school technology devices. Damage includes, but is not limited to broken screens, cracked casing, inoperability, water damage, etc.

If the CVUSD-owned device is damaged, lost, stolen or fails to be returned to CVUSD, it may result in the device reported stolen to the Thousand Oaks Police Department.

Chromebook Insurance

CVUSD is coordinating with U-PIC Insurance Services (**School Device Coverage**), to offer insurance for District issued Chromebooks.

Information regarding the insurance purchase process will be communicated at the start of the school year. The insurance policy is good for one year, and covers provides full coverage for accidental damage, loss, theft and

perils (flood, fire & vandalism). The policy also covers lost or stolen AC adapters/charging cables (limit of 1 charger per policy).

Bring Your Own Device (BYOD)

BYOD is an option made available to students, which allows them to bring their privately owned portable technology devices such as laptops, tablets, smart phones, etc. to school for academic use.

Bringing privately owned devices to school is completely optional. Although research shows that personal computing devices effectively engage students in the learning process, a student's learning experience will not be adversely affected by not bringing a device to school.

CVUSD makes every effort to ensure our wireless network meets industry standards and is designed to support the majority of 802.11 standards. CVUSD cannot guarantee compatibility with every device that attempts to connect to the WiFi network. In the event a personal device is determined not compatible with the CVUSD network a District provided 1:1 device will be available. This policy outlines appropriate use and prohibited activities for BYOD devices.

BYOD Guidelines

Each CVUSD classroom teacher will, at his/her discretion, implement and communicate the BYOD rules and expectations for the classroom. For example, some teachers may request that students refrain from smart phone use during class. The following protocols are provided to parents and students as a guideline of expectations and opportunities only:

- Students may bring devices that fit into the following categories: laptops, netbooks, tablets/iPads, and smartphones.
- Devices are to be used only during specified times during the instructional period. These times are designated by the child's teacher, school administrator, or other District and site staff members.
- There should be no expectation of printing student documents directly from a student BYOD.

Proper Care of BYOD

Student use of technology in the classroom is considered a privilege at CVUSD. Students are expected to exercise responsible behavior when handling technology, including personally owned devices and the devices of others. This behavior includes but is not limited to the following.

- Any devices brought to school should be brought in a protective case or sleeve to limit the potential for damage to the device.
- Limit device exposure to direct sunlight.
- Never leave a device unattended, both in and out of the classroom.
- Keep the device away from water and other liquids, such as sprinklers, rain, puddles, and beverages.
- Any devices, for which anti-virus software is available, must have an up-to-date version of the antivirus software running.

BYOD: Logging In, Connecting to the Network, and Basic Troubleshooting

Each student is expected to use his/her own District-provided Google account (*example: 123456@learn.conejousd.net*) username and password to access the CVUSD WiFi network via any student or family-owned devices. CVUSD makes every reasonable effort to ensure that the WiFi network (at available schools) remains in proper working order and is available to students for connection via BYOD. However, the nature of

modern technology lends itself to occasional down time. In the interest of best supporting classroom instruction, see the basic troubleshooting tips that are listed in Classroom and Take-Home Devices section.

CVUSD Liability for Parent and Student-Owned (BYOD)

Student and family technology brought to school remains the sole property of the student and therefore will not receive direct technical support from CVUSD technology staff. As such, any technical support for the device must be provided by the student and family.

CVUSD makes every reasonable effort to maintain a safe learning environment for all students. CVUSD assumes no responsibility for damage, loss, or theft of devices a student brings to school. As with any other student property, devices brought to school from home are the student's responsibility. It is recommended that families stress the important responsibilities students have when bringing their devices to school.

Instructional Software

CVUSD, through a thoughtful and innovative environment, encourages the use of instructional software by staff and students. As the District works to fulfill its mission of preparing students for the future, we will increasingly utilize tools and resources that are online and accessed through the Internet. Although not all instructional software requires a student online account, online accounts are necessary to access some web-based content and collaboration tools such as Google Drive, Google Classroom, as well as other educational online resources. These web and cloud-based services permit online distribution and submission of student assignments, online class discussions and collaboration activities, web-based curriculum or learning resources, and student communication.

All instructional software that utilizes student accounts or data of any kind will be in compliance with applicable federal and state requirements. District-provisioned student accounts will be in compliance with requirements including the Children's Online Privacy Protection Act (COPPA) and the Student Online Personal Information Protection Act (SOPIPA - California SB1777, AB1442, and AB1584).

CVUSD has partnered with CITE.org (California Information Technology in Education) and CSPA (California Student Privacy Alliance) to execute privacy agreements for all software and web-based tools used in student learning. This process ensures that CVUSD vendors remain compliant with all applicable state and federal laws and regulations related to student data protection.

Copies of executed Student Data Privacy Agreements between CVUSD and vendors are available here: https://sdpc.a4l.org/district_search.php?districtID=2700&state=CA

Parents and guardians may obtain an Online Accounts Creation Opt-Out Form from their school office and submit it to the school principal to request that the District does not create online accounts for their student. If the District does not receive an opt-out form from a child's parent or guardian, the District will consider that as permission to create and manage student accounts used to access online resources as part of the annual submission of the Student Technology Acceptable Use Agreement.

If you choose to opt out, please consider speaking with your child's teachers to discuss alternatives to online lessons and assignments.