VICTOR VALLEY UNION HIGH SCHOOL DISTRICT

16350 Mojave Drive, Victorville, CA 92395-3655

760.955.3201

STUDENT ACCEPTABLE USE POLICY

Student Acceptable Use Policy and Guidelines

The Victor Valley Union High School District (VVUHSD) has implemented technology in all areas of the school environment. Excellence in education requires that technology is seamlessly integrated throughout the instructional program. The individual or collaborative use of classroom and take-home devices is one strategy to empower students to maximize their full potential, as well as prepare them for college and career.

To this end, VVUHSD provides a wide range of technology resources for student use within the classroom and at home. 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, as well as any directions or guidelines given by VVUHSD teachers, substitutes, administrators, and staff.

Mandatory Review

To educate students on expectations for responsible use of the VVUHSD electronic network, students are required to review this agreement each school year. Additionally, employees supervising students who use the VVUHSD electronic network shall provide training emphasizing its appropriate use. All District students shall acknowledge receipt and understanding of this Agreement and shall agree in an electronic form to comply with the same. The parent/legal guardian will also be notified of student responsibilities.

General Policies

- The VVUHSD electronic network has been established for specific educational purposes and for District business. The term "educational purpose" includes, but is not limited to, classroom activities, career development, and high-quality self-discovery activities.
- The VVUHSD electronic network has been established for educational purposes and not as a public access service or a public forum. Victor Valley Union School District has the right to place reasonable restrictions on material that is accessed or posted throughout the network.
- A content filtering solution is in place to prevent access to visual depictions that are obscene, pornographic, inappropriate for students, or harmful to minors, as defined by the Children's Internet Protection Act (CIPA).
- This Agreement also pertains to users who connect via non-District network services (e.g., cell phones, mobile hotspots, etc.) while on District property or while participating in school-related functions. However, VVUHSD cannot be held responsible for content accessed through such services.

- Students must sign and adhere to this Agreement, and parent/guardian permission is required for all students under the age of 18. The District is not responsible for the actions of students who violate this Agreement. Access is a privilege — not a right.
- The District reserves the right to monitor all activity on the VVUHSD electronic network. Students have no expectation of privacy with respect to usage of the electronic network, even if the use is for personal purposes.
- Students may be held responsible for any damage that is caused by their inappropriate use of the network or equipment.
- In addition to this Agreement, students are expected to follow all aspects of the Student Use of Technology Policy (BP 6163.4) and Student Use of Technology Administrative Regulation (AR 6163.4). The same rules, good manners, guidelines, and laws that are used with other daily school activities also apply in students' use of the VVUHSD electronic network.

Digital Citizenship Expectations

While utilizing any portion of the VVUHSD electronic network and equipment, students are expected to exhibit responsible behavior and refrain from engaging in inappropriate use. The VVUHSD electronic network is considered a limited forum, and therefore the District may restrict a student's use of the network for valid reasons, including but not limited to, violations of the following:

- Students shall not post information that, if acted upon, could cause damage or danger of disruption to the educational environment for staff and/or students.
- Students shall not engage in electronic personal attacks that are in violation of District policy or State or Federal law.
- Students shall not harass, bully, or engage in any activities intended to harm (physically or emotionally) another person. Harassment is persistently acting in a manner that distresses or annoys another person, and includes, but is not limited to online impersonation, intimidation, or denigration; sending persistent and unsolicited messages; cyber stalking, and changing or manipulating the digital property of others.
- Students shall not distribute or post fabricated, harmful, or defamatory information about a person or organization.
- Students shall not use the VVUHSD electronic network or equipment or personal devices to engage in criminal activity.
- Students shall not display, access, or send offensive, explicit, or inappropriate messages or content.
- Students shall not offer, provide, or purchase products or services through the VVUHSD electronic network.
- Students shall not use the VVUHSD electronic network for political lobbying.

Internet and Student Websites

- Access to Web-based resources is intended for educational purposes. Students are expected to adhere to responsible use guidelines as specified in this Agreement and District policy, and immediately report inappropriate sites to District staff.
- The use of any photographs or student work on any web pages must follow District guidelines established by the Communications Department.

- Material (graphics, text, sound, etc.) placed on any webpages are expected to meet academic standards of proper spelling, grammar, mechanics, the accuracy of the information, and legal standards of copyright.
- All student webpages must have a link back to the homepage of the classroom, school, or district, as appropriate.

Electronic Communication

- Students may be provided with accounts that allow for email, messaging, chat, social networking, etc. These accounts are to be used for specific educational purposes or activities in accordance with State and Federal law.
- Students shall not establish or access personal accounts through the District network for non-educational purposes.
- Students shall not repost content, including but not limited to pictures, messages, or videos, that were sent to them privately without the permission of the sender and any subjects depicted in the content.
- Students shall not post private and/or personal information about another person, including, but not limited to contact or identifier information.

Real-time, Interactive Communication Areas and Social Media

- Students may use District-supported chat, instant messaging, and/or social media in a moderated environment established to support educational purposes.
- When using social media resources (e.g., YouTube, threaded discussion groups, and blogs) for educational purposes, students are expected to comply with all aspects of the Student Use of Technology Policy (BP 6163.4), Student Use of Technology Administrative Regulation (AR 6163.4), and this Agreement.

Personal Safety

- Students shall not share personal contact and/or identifier information about themselves or other people. Personal contact/identifier information includes, but is not limited to, address, telephone, school address, email address, or Social Security Number.
- Students shall not disclose personal contact information, except to education institutes for educational purposes, companies, or other entities for career development purposes, or without specific authorization.
- Students shall not agree to meet with someone they have met online.
- Students shall promptly disclose to a teacher or other school employee any message received that is inappropriate or makes the student feel uncomfortable.

Care of Equipment

- Students must take care of the technology-focused equipment, which can be viewed as a privilege.
- Users may not remove network cables, keyboards, or any other components.
- Students may not modify the configuration or content of software installed on any District technology.
- Damages to technology may result in a charge being placed on the user's account.
- The District reserves the right to monitor, inspect, copy, and review district-owned devices.

System Security

- Students are responsible for their individual accounts and should take all reasonable precautions to prevent others from being able to use them, which includes, but is not limited to keeping passwords private.
- Students shall immediately notify a teacher or other school employee if they have identified a possible security problem. Students should not go looking for security problems, because this may be construed as an illegal attempt to gain access.
- Students shall not attempt to gain unauthorized access to any portion of the VVUHSD electronic network. This includes attempting to log in through another person's account or accessing another person's folders, work, or files. These actions are illegal, even if only for the purposes of "browsing".
- Students shall not attempt to access non-student District systems.
- Students shall not make deliberate attempts to disrupt the VVUHSD electronic network or destroy data by spreading computer viruses or by any other means. These actions are illegal.
- Students shall not intentionally attempt to access websites blocked by District policy, including the use of proxy services, VPN, software, or websites.
- Students shall not use sniffing or remote access technology to monitor the network or other user's activity.

Software and Files

- Software is available to students to be used as an educational resource. Students shall not install, upload or download the software without District permission. Any software that causes disruption to the VVUHSD electronic network will be removed.
- Files stored on the VVUHSD electronic network are treated in the same manner as other school records. Routine maintenance and monitoring of the VVUHSD electronic network by authorized employees may lead to the discovery that a student has violated this Agreement or the law. Students should not expect that files stored on District servers or accessed through the VVUHSD electronic network are private.

Technology Hardware

- Hardware and peripherals are provided as tools for student use for educational purposes. Students are not permitted to install or relocate network hardware and/or peripherals (except for portable devices), or to modify settings to equipment without the consent of the District Information Technology Department.
- Students shall not connect any unauthorized wired or wireless devices to the VVUHSD electronic network.

Vandalism

- Any malicious attempt to harm or destroy data, the network, other network components connected to the network backbone, hardware, or software may result in the cancellation of network privileges. Appropriate disciplinary action will be taken.

Plagiarism and Copyright Infringement

- Students may access copyrighted material for educational purposes.
- All students are expected to follow existing copyright laws. Posting any material (graphics, text, sound, etc.) that is in violation of any federal or state law is prohibited. This includes, but is not limited to, confidential information, copyrighted material, threatening or obscene material, and computer viruses.
- Copyrighted material shall not be placed on any system without the author's permission. Permission may be specified in the document, on the system, or must be obtained directly from the author.
- Students shall not plagiarize works found on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were original work.
- Students shall appropriately cite materials referenced or used in the production of original work.

Use of Artificial Intelligence (A.I.)

Overview

- In recognition of the rapid growth of artificial intelligence (AI) technologies and their potential to enhance educational experiences, VVUHSD is committed to facilitating the responsible and effective use of AI tools within our schools.

Definitions

- Artificial Intelligence (AI): Computer systems or software that perform tasks requiring human intelligence, including but not limited to learning, decision-making, and language processing.
- Large Language Models (LLMs): A type of AI that processes and generates human-like text based on vast amounts of data. LLMs can understand, converse, translate, and create content in natural language.
- Machine Learning: A subset of AI that involves computers learning from data without being explicitly programmed for specific tasks.
- Natural Language Processing (NLP): AI's ability to understand and generate human language.
- Generative AI: AI technologies that can generate new content, including text, images, audio, and video, based on their training data. These tools can be used for creative and educational purposes but must be used with consideration for accuracy, appropriateness, and originality.

Access and Permissions

- Access to approved AI tools is granted to students, faculty, and staff for educational and administrative purposes only.

Ethical Use

- Users must not employ AI tools to conduct or support cheating, plagiarism, or any academic dishonesty.
- Users must not employ AI tools to automate decision making without human oversight. The district believes in the Always Center Educators (ACE) model promoted by the United States Department of Education. Any output of artificial intelligence or machine learning will be limited to suggestions and recommendations—final decisions must be made by human beings with the appropriate review, nuance, and context.
- Generative AI content that is inappropriate, offensive, or harmful is strictly prohibited.
- Respect and courtesy must be maintained when interacting with AI systems, recognizing their impact on the learning environment.
- Users should be aware of the potential for AI bias in tools and consider this when interpreting AI-generated information or content. The district encourages critical thinking and scrutiny of AI outputs and training data

Privacy, Security, and Data Protection

- Users must be aware of data privacy concerns with AI tools, especially regarding the handling of personal and sensitive information.
- Personally identifiable, confidential, and/or sensitive information should never be shared with an AI tool unless such sharing is explicitly approved by the district.
- All AI tools must comply with the Family Educational Rights and Privacy Act (FERPA), the Children's Online Privacy Protection Act (COPPA), and other relevant privacy laws.
- The district ensures that AI tools employed have robust security measures to protect user data from unauthorized access.
- Users are expected to be aware of and comply with the terms and conditions of all AI tools, specifically with respect to age requirements. The district technology department maintains a list of minimum age and parental consent rules.
- Users are responsible for securing their accounts and personal information when using AI tools.
- The district conducts regular security assessments of AI technologies to safeguard against vulnerabilities.

Academic Integrity

- AI tools should supplement the educational process without undermining the integrity of academic work. Examples of appropriate use include generating ideas for brainstorming sessions, providing tutoring in specific subjects, and automating administrative tasks.
- Direct submission of AI-generated work as one's own without proper attribution or reliance on AI for completing assignments without understanding the content is prohibited.
- Users must respect copyright laws and intellectual property rights when using AI tools. This includes not using AI to replicate or modify copyrighted materials without authorization and properly citing all sources of content, including AI-generated content, to avoid plagiarism.

Videoconferencing/Classroom Video Feed

- All video conferencing must be for educational purposes.
- Students shall not record or stream classroom or other school-related activities without proper authorization. All such recordings or streaming must be in compliance with student privacy laws.

Due Process

- The District's authorized representatives will cooperate fully with local, state, or federal officials in any investigation related to any illegal activities conducted through the VVUHSD electronic network.
- Disciplinary actions will be tailored to meet specific concerns related to the violation. Violations of this Agreement may result in a loss of access as well as other disciplinary and/or legal action.

Limitation of Liability

- The District makes no guarantee that the functions or the services provided by or through the VVUHSD electronic network will be error-free or without defect. The District will not be responsible for any damage suffered, including but not limited to, loss of data, damage to personal devices, or interruptions of service.
- The District is not responsible for the accuracy or quality of the information obtained through or stored on the VVUHSD electronic network. The District will not be responsible for financial obligations arising through the unauthorized use of the network.
- The District utilizes a content filtering solution to block access to objectionable and inappropriate material on the Internet. Preventing all such access is impossible, however, and a risk exists that a student may access material intended only for adults, even with filtering in place. No safeguard is foolproof, and the District is not responsible for material encountered on its electronic network which may be deemed objectionable to a user or his/her parent/legal guardian.

Violations of This Agreement

Violations of this Agreement may result in loss of access as well as other disciplinary and/or legal action. Students' violation of this Agreement shall be subject to the consequences as indicated within this Agreement as well as other appropriate disciplinary action(s), including but not limited to:

- Use of VVUHSD electronic network only under the direct supervision
- Suspension of network privileges
- Revocation of network privileges
- Suspension of computer privileges
- Suspension from school
- Expulsion from school
- Legal action and prosecution by the authorities

Federal and state laws related to cybercrimes

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 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).

VVUHSD - Student Responsible Use Pledge

VVUHSD provides computers, internet access, and other technology resources for educational use. In accepting the responsibility of being issued access to VVUHSD technology resources, students are expected to abide by the following pledge:

As a student, I will practice good digital citizenship when using these technology resources. Good digital citizenship is good citizenship. I understand that I must act appropriately and follow these rules in order to be a good digital citizen, and I realize that I can be disciplined if I do not follow these guidelines and use computers and the internet inappropriately.

Respect and Protect Myself

- ✓ I understand that school computer files, email, and internet use are not private and can be monitored by teachers or administrators.
- ✓ I understand that I must not give my password or username to anyone and will not use, or attempt to use, other people's usernames and passwords.
- ✓ It is my responsibility to stay safe on the internet. I will not share personal information about myself or others like home address, phone numbers, passwords, personal photos, or Social Security numbers.
- ✓ I will not meet with anyone I met on the internet. I will tell parents, teachers, or administrators immediately if someone asks to meet me.
- ✓ I will not attempt to access inappropriate, profane, or obscene material. If I do so accidentally, I will not share it with other students and will notify a teacher or administrator right away.

Respect and Protect Others

- ✓ I will use the computer and internet-only with the teacher's permission and for the purpose that the teacher requested.
- ✓ I will respect copyright laws, not copy material without permission, and I will make sure to show where I found my information.
- ✓ I will be polite and show respect online. I will never cyberbully others. I will not harass, insult, or attack others.
- ✓ I will not send or display offensive messages or pictures or use obscene language in messages.

Respect and Protect Property

- ✓ I will respect and take good care of the devices/equipment and technology resources I use.