

Covina-Valley Unified School District

Student Internet and Technology Acceptable Use Policy

Introduction

The Covina-Valley Unified School District provides students with access to the Internet to promote educational goals and objectives and to enhance learning through the use of technology and resource sharing. Schools have rules for acceptable behavior. Because Internet access is used as part of a school activity, the school's code of conduct applies to Internet activities. The Internet and Technology Acceptable Use Policy is an extension of the school's behavior code. This Policy was developed to inform students of the appropriate, ethical, safe, and courteous use of the Internet and other school technology resources. It is important that students understand their use of the Internet is a privilege, not a right, and such use is for education purposes only. Before students can access the Internet from school, students and teachers will discuss appropriate behavior and guidelines for Internet use. If students do not follow these guidelines, they may lose access privileges and be subject to disciplinary action.

Parents and students are advised the District does not have control over the information on the Internet; however, the District does comply with state and federal guidelines for preventive filtering. Despite all filtering efforts, Internet sites may contain material that is inaccurate, prohibited, or potentially offensive to some people. Teachers will provide instruction on Internet safety and search skills to promote optimal and safe Internet experiences for students.

The District supports and respects each family's right to decide whether their child(ren) should access the District Internet while at school. The parent or guardian who signs the Consent and Waiver Statement at the end of this Policy gives permission for their child to access the Internet at school. In addition, by signing, parents and students acknowledge they are aware of the acceptable behaviors for using District Internet access. This signed statement will be kept on file in the school's office.

Student Safety Awareness

Teachers will attempt to ensure student safety when their students access the District's Internet. Teachers must be familiar with this Policy and will monitor student Internet use to support student safety. Teachers will provide grade-appropriate instruction on digital citizenship. Instruction will include: cyberbullying, cyber-awareness, legal issues, consequences, and response mechanisms. When using the Internet or email to communicate with others, students should be reminded:

- The identity of individuals who post web pages or communicate over the Internet is unknown.
- Individuals may provide inaccurate or misleading information through Internet communications.
- Information posted on or shared through the Internet *is not private*. All users must think carefully before communicating online.
- Students may not give out anyone's personal or contact information, including telephone numbers and addresses, through the District's Internet.
- Students must never arrange to meet strangers they communicate with online.

Covina-Valley Unified School District
Student Internet and Technology Acceptable Use Policy

If a student thinks a website or information on the Internet violates this Policy, the student should immediately inform the teacher. The teacher will notify the Technology Systems Services (TSS) Department so the filtering mechanism may be amended.

Personal Use

District technology, networks, and Internet connections, including District-authorized websites, are operated by the District for educational purposes, and may be used only for those purposes consistent with this Policy and the mission and goals of the District. By permitting this limited use of its technology, the District does not intend to create a limited public forum or otherwise guarantee an individual right to free speech. District email accounts may be used only for school-related purposes. The Internet and computer networks may not be used for personal or non-school related purposes. Communications through District-owned technology or the District's Internet connection must comply with all District policies and regulations.

Personal Technology

Students may bring authorized personal digital devices to school to support instruction and learning, as part of the Bring Your Own Device (BYOD) Program. Students are not required to bring a personal device to school but instead may use school equipment. No student will be left out of the instruction process as a result of not having a personally owned device. Not all teachers allow use of personal devices in class, so it is important for students to know their teachers' expectations.

All students participating in this program must have a complete signed Consent and Waiver Statement on file prior to bringing a personal device on campus. Students must comply with this Policy and District policies and regulations when using personal devices on District property.

Students and parents/guardians are responsible for the maintenance and repair of the students' personal electronic devices, including any software or hardware issues that arise while the device is connected to the District network. The District is not liable for loss, damage, misuse, or theft of any personal electronic device.

Any student who uses a personal electronic device in violation of law, Board policy, administrative regulation, or this Policy is subject to discipline and may be referred to law enforcement as appropriate.

Applications Policy

To maximize the use of instructional technology tools, teachers and students will be provided access to various educational services including as examples: Discovery Streaming, Haiku Learning, Google Apps for Education, YouTube, and blogs. These services allow teachers and students to collaborate on assignments, communicate, and extend learning beyond the school day.

Privacy

Computer files and communications over the District's systems, including email, are not private and students do not have a right to privacy in such information. To ensure proper use of District technology, the Superintendent or designee may monitor or audit use of the District's

Covina-Valley Unified School District
Student Internet and Technology Acceptable Use Policy

technological resources, including but not limited to, network transmissions, system files, and email, at any time for any reason without advance notice or consent.

Harassment/Discrimination/Cyberbullying/Inappropriate Communication

Students may not access, post, or display harmful or inappropriate matter that is threatening, obscene, disruptive, or sexually explicit, or that can reasonably be construed as harassment or disparagement of others based on their race/ethnicity, national origin, sex, gender, sexual orientation, age, disability, religion, or political beliefs. Harmful matter includes matter, taken as a whole, and with respect to minors, that appeals to the prurient interest and depicts or describes, in a patently offensive way, sexual conduct and lacks serious literary, artistic, political, or scientific value for minors. (20 U.S.C. 6777; California Penal Code 313)

Use of technology to harass, threaten, demean, humiliate, intimidate, embarrass, or annoy others is unacceptable and will not be tolerated. This type of behavior is known as cyberbullying and is subject to disciplinary action.

Cyberbullying includes the transmission of communications, posting of harassing messages, direct threats, or other harmful texts, sounds, or images on the Internet, social networking sites, or other digital technologies using a telephone, computer, or any wireless communication device, camera, computer, or pager. Cyberbullying also includes breaking into another person's electronic account and assuming that person's identity in order to damage that person's reputation. (Education Code 48900(r))

Inappropriate communication includes, but is not limited to: obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language or images captured, typed, posted, or spoken by students; information that could cause damage to an individual or the school community or create the danger of disruption of the academic environment; personal attacks, including prejudicial or discriminatory attacks; harassment (persistently acting in a manner that distresses or annoys another person) or stalking of others; knowingly or recklessly posting false information about a person or organization; and communication that promotes the destruction of property, including the acquisition or creation of weapons or other destructive devices. If a student is told to stop sending communications, the student must cease the activity immediately.

Attempting to disable or override District Internet filters so as to access harmful or prohibited material is prohibited and will result in immediate suspension or revocation of access privileges.

Misuse of Internet Access

In order for all students to have equitable access to school technology resources, students:

- Must use District technology and Internet access only for educational purposes.
- May download or print only information needed for assignments as authorized by the teacher.
- May access email and communication programs with the teacher's prior authorization.
- May not access Internet or computer games without the teacher's prior authorization.

Web Pages and Social Media

Web pages can provide a means for students to communicate and share data with others around the world. The District recognizes that students may utilize various social media websites

Covina-Valley Unified School District

Student Internet and Technology Acceptable Use Policy

(including, but not limited to, YouTube, Facebook, Twitter, Pinterest, and Google+) for educational purposes such as online collaboration and class assignments. Students may be assigned to post web pages related to curricular projects. Student-developed web pages that are posted by the school or District must be authorized and approved by school site teacher(s) or administrator. It is important that students realize that they represent their school when posting web page information on a District-authorized web site. All web pages created on or through the use of District computer systems are District property subject to District monitoring and editing. All pages, posts, or sites created through the use of District technology or property must be related to a curricular project or District business. All users of the District's social media platforms must adhere to applicable policies.

The Covina-Valley Unified School District and its school names may not be used, cited, or claimed as web hosts, without prior written authorization from the District office.

Student Photographs and Videos on School and District Web Pages

Students may not post unauthorized photos or videos of other students on their school-related web pages. Because of the wide accessibility of the Internet and potential risk to students, photographs of individual students must not be published with their names or other personally identifiable information without the prior written consent of the student's parent/guardian. Therefore, display of any student images on web pages is permitted only under the direction of the responsible teacher.

Plagiarism

Plagiarism is taking ideas or writings from another person and offering them as one's own. Transmission of material that plagiarizes another's work is prohibited. Credit must always be given to the person who created the information or the idea. A student who leads readers to believe they are reading the student's original work, when it is not, is guilty of plagiarism. Cutting and pasting another's ideas into a document is very easy to do, but is unethical if the work is not quoted or cited properly. When referencing someone else's work, students must provide citations so the author is given credit. This way, the teacher will know which ideas are those of the student and which belong to someone else. Under some circumstances students may download limited amounts of copyrighted material for school use under "fair use" provisions of copyright law (see <http://www.loc.gov/teachers/copyrightmystery>).

Illegal Downloads and Installs

Students may not download, copy, or sell an illegal copy of any commercially copyrighted or licensed software, music, film, or other media at school or through District technology resources. Students may not install software or plug-ins onto any school computer. Violation of this provision will result in immediate suspension or revocation of access privileges.

Legal and Disciplinary Issues

California law makes it a felony to intentionally access any computer system or network for the purpose of: devising or executing any scheme or artifice to defraud or extort or obtaining money, property, or services with false or fraudulent intent, representations, or promises.

Covina-Valley Unified School District
Student Internet and Technology Acceptable Use Policy

It is also a felony to maliciously access, alter, delete, damage or destroy technology resources, networks, computer programs, or data. Anyone committing acts of this kind will face disciplinary action by the school and referral to the appropriate law enforcement officials.

Students may not:

- Use District technology resources or networks for illegal activity, including violation of institutional or third-party copyright, license agreements, and other contracts;
- Disrupt information network traffic or crash the network and connected systems;
- Attempt to degrade or to disrupt equipment or system performance;
- Use District computing resources for commercial or financial gain or fraud, or to distribute unsolicited advertising;
- Steal data, equipment, or intellectual property;
- Gain unauthorized access to the files of others or vandalize the data or files of another user;
- Gain or attempt to gain unauthorized access to school or District data, resources, or entities; or
- Attempt to read, delete, copy, modify, use, or forge another user's email or email identity.

Consequences of Violations

Administrators will utilize the District's Discipline Policy Statements when determining the level of infraction and its consequences. Violations may result in, without limitation:

- Suspension or revocation of Internet and District network access and network privileges;
- Suspension or revocation of computer access;
- School suspension or expulsion;
- Financial liability for damage; and
- Referral to law enforcement for possible criminal prosecution.

Additional Notices and Disclaimers

The District reserves the right to delete, without notice, from its network system any email messages or any material from school, class, or student web pages it deems inappropriate as defined by this Policy or other school behavioral guidelines.

The District's specific technology conditions and services will change from time to time. The District has the right to restrict or terminate computer, Internet, and District network access at any time for any reason and to change the terms and conditions of this Policy. Any changes will be sent to students and parents/legal guardians for their signature.

The District makes no warranties with respect to its Internet access, and specifically assumes no responsibilities for:

- The content of any advice or information received by a student from a source outside the District, or any costs or charges incurred as a result of seeing or accepting such advice;
- Any costs, liability or damages caused by the way the student chooses to use his or her District Internet and District network access; and

Covina-Valley Unified School District
Student Internet and Technology Acceptable Use Policy

- Any damages that occur from using the District's Internet access, including consequences of service interruptions or changes, even if these disruptions arise from circumstances under the control of the District.