STUDENT USE OF TECHNOLOGY

The Governing Board intends that technological resources provided by the district be used in a safe and responsible manner in support of the instructional program and for the advancement of student learning. All students using these resources shall receive instruction in their proper and appropriate use.

(cf. 0440 - District Technology Plan)
(cf. 1113 - District and School Web Sites)
(cf. 1114 - District-Sponsored Social Media)
(cf. 4040 - Employee Use of Technology)
(cf. 6163.1 - Library Media Centers)

Teachers, administrators, and/or library media specialists are expected to review the technological resources and online sites that will be used in the classroom or assigned to students in order to ensure that they are appropriate for the intended purpose and the age of the students.

The Superintendent or designee shall notify students and parents/guardians about authorized uses of district technology, user obligations and responsibilities, and consequences for unauthorized use and/or unlawful activities in accordance with this Board policy and the district's Acceptable Use Agreement.

District technology includes, but is not limited to, computers, the district's computer network including servers and wireless computer networking technology (wi-fi), the Internet, email, USB drives, wireless access points (routers), tablet computers, smartphones and smart devices, telephones, cellular telephones, personal digital assistants, pagers, MP3 players, wearable technology, any wireless communication device including emergency radios, and/or future technological innovations, whether accessed on or off site or through district-owned or personally owned equipment or devices.

Before a student is authorized to use district technology, the student and his/her parent/guardian shall sign and return the Acceptable Use Agreement. In that agreement, the parent/guardian shall agree not to hold the district or any district staff responsible for the failure of any technology protection measures or user mistakes or negligence and shall agree to indemnify and hold harmless the district and district staff for any damages or costs incurred.

(cf. 6162.6 - Use of Copyrighted Materials)

The district reserves the right to monitor student use of technology within the jurisdiction of the district without advance notice or consent. Students shall be informed that their use of district technology, including, but not limited to, computer files, email, text messages, instant messaging, and other electronic communications, is not private and may be accessed by the district for the purpose of ensuring proper use. Students have no reasonable expectation of privacy in use of the district technology. Students' personally owned devices shall not be searched except in cases where there is a reasonable suspicion, based on specific and objective facts, that the search will uncover evidence of a violation of law, district policy, or school rules.

(cf. 5145.12 - Search and Seizure)

STUDENT USE OF TECHNOLOGY (continued)

The Superintendent or designee may gather and maintain information pertaining directly to school safety or student safety from the social media activity of any district student in accordance with Education Code 49073.6 and BP/AR 5125 - Student Records.

(cf. 5125 - Student Records)

Whenever a student is found to have violated Board policy or the district's Acceptable Use Agreement, the principal or designee may cancel or limit a student's user privileges or increase supervision of the student's use of the district's equipment and other technological resources, as appropriate. Inappropriate use also may result in disciplinary action and/or legal action in accordance with law and Board policy.

(cf. 5125.2 - Withholding Grades, Diploma or Transcripts)
(cf. 5144 - Discipline)
(cf. 5144.1 - Suspension and Expulsion/Due Process)
(cf. 5144.2 - Suspension and Expulsion/Due Process (Students with Disabilities))

The Superintendent or designee, with input from students and appropriate staff, shall regularly review and update procedures to enhance the safety and security of students using district technology and to help ensure that the district adapts to changing technologies and circumstances.

Internet Safety

The Superintendent or designee shall ensure that all district computers with Internet access have a technology protection measure that protects against access to visual depictions that are obscene, child pornography, or harmful to minors and that the operation of such measures is enforced. (20 USC 7131; 47 USC 254; 47 CFR 54.520)

To reinforce these measures, the Superintendent or designee shall implement rules and procedures designed to restrict students' access to harmful or inappropriate matter on the Internet and to ensure that students do not engage in unauthorized or unlawful online activities.

Harmful matter includes matter, taken as a whole, which to the average person, applying contemporary statewide standards, appeals to the prurient interest and is matter which depicts or describes, in a patently offensive way, sexual conduct and which lacks serious literary, artistic, political, or scientific value for minors. (Penal Code 313)

The district's Acceptable Use Agreement shall establish expectations for appropriate student conduct when using the Internet or other forms of electronic communication, including, but not limited to, prohibitions against:

1. Accessing, posting, submitting, publishing, or displaying harmful or inappropriate matter that is threatening, obscene, disruptive, or sexually explicit, or that could 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

STUDENT USE OF TECHNOLOGY (continued)

(cf. 5131 - Conduct)
(cf. 5131.2 - Bullying)
(cf. 5145.3 - Nondiscrimination/Harassment)
(cf. 5145.7 - Sexual Harassment)
(cf. 5145.9 - Hate-Motivated Behavior)

2. Intentionally uploading, downloading, or creating computer viruses and/or maliciously attempting to harm or destroy district equipment or materials or manipulate the data of any other user, including so-called "hacking"

3. Distributing personal identification information, including the name, address, telephone number, Social Security number, or other personally identifiable information, of another student, staff member, or other person with the intent to threaten, intimidate, harass, or ridicule that person

The Superintendent or designee shall provide age-appropriate instruction regarding safe and appropriate behavior on social networking sites, chat rooms, and other Internet services. Such instruction shall include, but not be limited to, the dangers of posting one's own personal identification information online, misrepresentation by online predators, how to report inappropriate or offensive content or threats, behaviors that constitute cyberbullying, and how to respond when subjected to cyberbullying.

Legal Reference:

EDUCATION CODE
49073.6 Student records; social media
51006 Computer education and resources
51007 Programs to strengthen technological skills
60044 Prohibited instructional materials
PENAL CODE
313 Harmful matter
502 Computer crimes, remedies
632 Eavesdropping on or recording confidential communications
653.2 Electronic communication devices, threats to safety
UNITED STATES CODE, TITLE 15
6501-6506 Children's Online Privacy Protection Act
UNITED STATES CODE, TITLE 20
7101-7122 Student Support and Academic Enrichment Grants
7131 Internet safety
UNITED STATES CODE, TITLE 47
254 Universal service discounts (E-rate)
CODE OF FEDERAL REGULATIONS, TITLE 16
312.1-312.12 Children's Online Privacy Protection Act
CODE OF FEDERAL REGULATIONS, TITLE 47
54.520 Internet safety policy and technology protection measures, E-rate discounts
COURT DECISIONS
New Jersey v. T.L.O., (1985) 469 U.S. 325

STUDENT USE OF TECHNOLOGY (continued)

Management Resources:

CSBA PUBLICATIONS
Cyberbullying: Policy Considerations for Boards, Policy Brief, July 2007
FEDERAL TRADE COMMISSION PUBLICATIONS
How to Protect Kids' Privacy Online: A Guide for Teachers, December 2000
WEB SITES
CSBA: http://www.csba.org
American Library Association: http://www.ala.org
California Coalition for Children's Internet Safety: http://www.cybersafety.ca.gov
Center for Safe and Responsible Internet Use: http://csriu.org
Federal Communications Commission: http://www.fcc.gov
Federal Trade Commission, Children's Online Privacy Protection: http://www.ftc.gov/privacy/privacyinitiatives/childrens.html
U.S. Department of Education: http://www.ed.gov

Policy
adopted: December 9, 1996
revised: June 23, 1998
revised: November 16, 1999
revised: June 26, 2001
revised: May 21, 2002
revised: January 9, 2007
revised: June 12, 2012
revised: October 23, 2018

VISALIA UNIFIED SCHOOL DISTRICT
Visalia, California

STUDENT USE OF TECHNOLOGY

The principal or designee shall oversee the maintenance of each school's technological resources and may establish guidelines and limits on their use. All instructional staff shall receive a copy of this administrative regulation, the accompanying Board policy, and the district's Acceptable Use Agreement describing expectations for appropriate use of the system and shall also be provided with information about the role of staff in supervising student use of technological resources. All students using these resources shall receive instruction in their proper and appropriate use.

(cf. 0440 - District Technology Plan)
(cf. 4040 - Employee Use of Technology)
(cf. 4131- Staff Development)
(cf. 4231 - Staff Development)
(cf. 4331 - Staff Development)

Teachers, administrators, and/or library media specialists shall prescreen technological resources and online sites that will be used for instructional purposes to ensure that they are appropriate for the intended purpose and the age of the students.

(cf. 6163.1 - Library Media Centers)

Online/Internet Services: User Obligations and Responsibilities

Students are authorized to use district equipment to access the Internet or other online services in accordance with Board policy, the user obligations and responsibilities specified below, and the district's Acceptable Use Agreement.

1. The student in whose name an online services account is issued is responsible for its proper use at all times. Students shall keep personal account numbers and passwords private and shall only use the account to which they have been assigned.

2. Students shall use the district's system safely, responsibly, and primarily for educational purposes.

3. Students shall not access, post, submit, publish, or display harmful or inappropriate matter that is threatening, obscene, disruptive, or sexually explicit, or that could 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.

(cf. 5131 - Conduct)
(cf. 5145.3 - Nondiscrimination/Harassment)
(cf. 5145.7 - Sexual Harassment)
(cf. 5145.9 - Hate-Motivated Behavior)

STUDENT USE OF TECHNOLGY (continued)

Harmful matter includes matter, taken as a whole, which to the average person, applying contemporary statewide standards, appeals to the prurient interest and is matter which depicts or describes, in a patently offensive way, sexual conduct and which lacks serious literary, artistic, political, or scientific value for minors. (Penal Code 313)

4. Unless otherwise instructed by school personnel, students shall not disclose, use, or disseminate personal identification information about themselves or others when using email, chat rooms, or other forms of direct electronic communication. Students also shall be cautioned not to disclose such information by other means to individuals contacted through the Internet without the permission of their parents/guardians.

   Personal information includes the student's name, address, telephone number, Social Security number, or other personally identifiable information.

5. Students shall not use the system to encourage the use of drugs, alcohol, or tobacco, nor shall they promote unethical practices or any activity prohibited by law, Board policy, or administrative regulations.

(cf. 3513.3 - Tobacco-Free Schools)
(cf. 5131.6 - Alcohol and Other Drugs)

6. Students shall not use the system to engage in commercial or other for-profit activities.

7. Students shall not use the system to threaten, intimidate, harass, or ridicule other students or staff.

8. Copyrighted material shall be posted online only in accordance with applicable copyright laws. Any materials utilized for research projects should be given proper credit as with any other printed source of information.

(cf. 5131.9 - Academic Honesty)
(cf. 6162.6 - Use of Copyrighted Materials)

9. Students shall not intentionally upload, download, or create computer viruses and/or maliciously attempt to harm or destroy district equipment or materials or manipulate the data of any other user, including so-called "hacking."

(cf. 5131.5 - Vandalism and Graffiti)

10. Students shall not attempt to interfere with other users' ability to send or receive email, nor shall they attempt to read, delete, copy, modify, or use another individual's identity.

STUDENT USE OF TECHNOLGY (continued)

11. Students shall report any security problem or misuse of the services to the teacher or principal.

The district reserves the right to monitor use of the district's systems for improper use without advance notice or consent. Students shall be informed that computer files and electronic communications, including email, are not private and may be accessed by the district for the purpose of ensuring proper use.

(cf. 5145.12 - Search and Seizure)

The principal or designee shall make all decisions regarding whether or not a student has violated Board policy or the district's Acceptable Use Agreement. The decision of the principal or designee shall be final. Inappropriate use may result in cancellation of the student's user privileges, disciplinary action, and/or legal action in accordance with law and Board policy.

(cf. 5144 - Discipline)
(cf. 5144.1 - Suspension and Expulsion/Due Process)
(cf. 5144.2 - Suspension and Expulsion/Due Process (Students with Disabilities))

Regulation
approved: December 9, 1996
revised: June 23, 1998
revised: November 16, 1999
revised: June 26, 2001
revised: May 21, 2002
revised: January 9, 2007
revised: June 12, 2012

VISALIA UNIFIED SCHOOL DISTRICT
Visalia, California

VISALIA UNIFIED SCHOOL DISTRICT
Acceptable Use Agreement
Student

The purpose of this Acceptable Use Agreement ("Agreement") is to ensure a safe and appropriate environment for all students. Providing and issuing a Chromebook or Chromebook with WiFi hotspot, or _____ ("Device") for instructional use to our students is an important part of our school's instructional program. This Agreement notifies parents and students about the acceptable ways in which Devices may be used. The Visalia Unified School District ("District") recognizes and supports advances in technology and provides an array of technology resources for students to use to enhance learning and education. While these technologies provide a valuable resource to students, it is important that students' use of technology be appropriate for school purposes.

Pursuant to Board Policy 6163.4, only Users of District Technology who submit a signature acknowledging receipt and agreement to the terms of use outlined in this Agreement and the District's Acceptable Use Agreement are authorized to use Devices.

Terms of Use

Acceptable Use: District students are only permitted to use Devices for purposes that are safe (pose no risk to students, employees or assets), legal, ethical, do not conflict with the mission of the District, and are compliant with all other District policies. Usage that meets these requirements is deemed "proper" and "acceptable" unless specifically excluded by this policy or other District policies. The District reserves the right to restrict online destinations through software or other means.

Removal or alteration of any District identification label attached or displayed on the Device is strictly prohibited. Users may not deface the Device or adhere stickers or any other markings to it.

Additionally, the District expressly prohibits:

1. Using Devices for commercial gain;
2. Altering or defacing the Device in any way;
3. Disassembling or attempting to repair the Device in any way;
4. Leaving the Device unattended in public or loaning out the device to other individuals;
5. Accessing Devices for the purpose of gaming or engaging in any illegal activity;
6. Using the Device to encourage the use of drugs, alcohol, or tobacco;
7. Transmission of confidential information to unauthorized recipients;
8. Inappropriate and unprofessional behavior online such as use of threats, intimidation, bullying or "flaming";
9. Accessing, posting, submitting, publishing, or displaying harmful or inappropriate matter that is threatening, obscene, disruptive, or sexually explicit;
10. Using Devices for the creation or distribution of chain emails, any disruptive or offensive messages, offensive comments about race, gender, disabilities, age, sexual orientation, religious beliefs/practices, political beliefs, or material that is in violation of workplace harassment or workplace violence laws or policies;
11. Significant consumption of Devices for non-school related activities (such as video, audio or downloading large files) or excessive time spent using Devices for non-school purposes (e.g. shopping, personal social networking, or sports related sites);
12. Knowingly or carelessly performing an act that will interfere with or disrupt the normal operation of computers, terminals, peripherals, or networks, whether within or outside of Devices (e.g., deleting programs or changing icon names) is prohibited;

VISALIA UNIFIED SCHOOL DISTRICT - ACCEPTABLE USE AGREEMENT – STUDENT (CONTINUED)

13. Distributing personal identification information, including the name, address, telephone number, Social Security number, or other personally identifiable information, of another student, staff member, or other person with the intent to threaten, intimidate, harass, or ridicule that person;
14. Infringe on copyright, license, trademark, patent, or other intellectual property rights;
15. Disabling any and all antivirus software running on Devices or "hacking" with Devices; or
16. Intentionally uploading, downloading, or creating computer viruses and/or maliciously attempting to harm or destroy district equipment or materials.

Distance Learning Use: Users agree to ensure the Device has a fully charged battery before class sessions. Internet surfing and YouTube cruising are strictly prohibited and will be monitored. Listening to personal music during instructional time is strictly prohibited. In the event a student is not able to access the internet to participate in distance learning, the District shall provide an alternate means of participation in the District curriculum.

Accountability: Users are prohibited from anonymous usage of Devices. In practice, this means users must sign in with their uniquely assigned District User ID before accessing/using Devices. Users may only use the school provided Google account, which may be reviewed at any time by any school administrator or teacher. Similarly, "spoofing" or otherwise modifying or obscuring a user's IP Address, or any other user's IP Address, is prohibited. Circumventing user authentication or security of any host, network, or account is also prohibited.

Disclaimer: The District cannot be held accountable for the information that is retrieved via the network. The District will not be responsible for any damages you may suffer, including loss of data resulting from delays, non-deliveries, or service interruptions caused by the District Systems, System Administrators or your own errors or omissions. Use of any information obtained is at your own risk. The District makes no warranties (expressed or implied) with respect to: (a) the content of any advice or information received by a student, or any costs or charges incurred as a result of seeing or accepting any information; or (b) any costs, liability, or damages caused by the way the student chooses to use his or her access to the network.

Password Policy: Passwords must not be shared with anyone and must be treated as confidential information. Passwords must be changed as often as required by the District's IT department. All Users are responsible for managing their use of Devices and are accountable for their actions relating to security. Allowing the use of your account or Device by another user is also strictly prohibited. All passwords created for or used on any Device are the sole property of the District. The creation or use of a password by a student on Devices does not create a reasonable expectation of privacy.

Responsibility: Users are responsible for their own use of Devices and are advised to exercise common sense and follow this Agreement in regards to what constitutes appropriate use of Devices in the absence of specific guidance. Users are responsible at all times for the care and appropriate use of the issued Device and must adhere to the terms of use each time the device is used, on or off school grounds. Users agree to ensure the Device is secure and safe at all times, and will handle the Device carefully and protect it from potential sources of damage. Devices should be treated like a textbook and are a tool to help in the learning process. Users may only use Devices as directed by teachers.

Revocation of Authorized Possession: The District reserves the right, at any time, for any reason or no reason, to revoke a User's permission to access, use, or possess Devices.

Restriction of Use: The District reserves the right, at any time, for any reason or no reason, to limit the manner in which a User may use Devices in addition to the terms and restrictions already contained in this Agreement.

Third-Party Technology: Connecting unauthorized equipment to the Device, including the unauthorized installation of any software (including shareware and freeware), is prohibited.

VISALIA UNIFIED SCHOOL DISTRICT - ACCEPTABLE USE AGREEMENT – STUDENT (CONTINUED)

Reporting: If a student becomes aware of any security problem (such as any compromise of the confidentiality of any login or account information) or misuse of Devices, he/she shall immediately report such information to the Superintendent or designee. Users must report theft (or suspected theft), loss, damage, or malfunction of the Device to school personnel immediately. The student's parent/guardian is required to notify police and provide a copy of an official police report to District administration, if a Device is reported as stolen outside of school grounds.

Inspection: Upon request, the student agrees to deliver the issued Device to District staff for technical inspection or to verify inventory or other information. Students will make available for inspection by any school administrator or teacher any messages, communication, or files sent or received on any District issued Device.

District Property: All Devices are property of the District. All such issued Devices shall be returned to the District prior to the conclusion of each school year or prior to the student's withdrawal from the District, if earlier than the conclusion of the school year.

Consequences for Violation: Violations of the law, Board policy, or this Agreement may result in revocation of a student's access to Devices and/or restriction of his/her use of Devices and/or discipline, up to and including suspension or expulsion. In addition, violations of the law, Board policy, or this Agreement may be reported to law enforcement agencies as deemed appropriate.

Discipline for Misuse or Damage: All discipline regarding the use of Devices will be evaluated in regards to the incident frequency, severity, and best possible course of action. The school Principal or Designee shall have the final say as to the disciplinary action taken in accordance with the California Education Code. Parents or guardians may be responsible for the full price of repair or replacement of the Device for willful damage or loss of the Device.

Enforcement

Record of Activity: Usage may be monitored or researched in the event of suspected improper Device usage or policy violations.

Blocked or Restricted Access: User access to specific Internet resources, or categories of Internet resources, deemed inappropriate or non-compliant with this policy may be blocked or restricted. A particular website that is deemed "Acceptable" for use may still be judged a risk to the District (e.g. it could be hosting malware), in which case it may also be subject to blocking or restriction.

No Expectation of Privacy: Users have no expectation of privacy regarding their use of Devices. Log files, audit trails and other data about user activities with Devices may be used for forensic training or research purposes, or as evidence in a legal or disciplinary matter. Users are on notice that Devices are subject to search and seizure in order to facilitate maintenance, inspections, updates, upgrades, and audits, all of which necessarily occur both frequently and without notice so that the District can maintain the integrity of Devices. All data viewed or stored is subject to audit, review, disclosure and discovery. Such data may be subject to disclosure pursuant to the Public Records Act (California Government Code section 6250, *et seq*.). Pursuant to the Electronic Communications Privacy Act of 1986 (18 USC 2510, *et seq*.), notice is hereby given that there are no facilities provided by Devices for sending or receiving private or confidential electronic communications. System Administrators have access to all email and will monitor messages. Messages relating to or in support of illegal or inappropriate activities will be reported to the appropriate authorities and/or District personnel.

VISALIA UNIFIED SCHOOL DISTRICT - ACCEPTABLE USE AGREEMENT – STUDENT (CONTINUED)

The District reserves the right to monitor and record all use of Devices, including, but not limited to, access to the Internet or social media, communications sent or received from Devices, or other uses within the jurisdiction of the District. Such monitoring/recording may occur at any time without prior notice for any legal purposes including, but not limited to, record retention and distribution and/or investigation of improper, illegal, or prohibited activity. Students should be aware that, in most instances, their use of Devices (such as web searches or emails) cannot be erased or deleted. The District reserves the right to review any usage and make a case-by-case determination whether the User's duties require access to and/or use of Devices which may not conform to the terms of this policy.

Specific Consent to Search and Seizure of District Technology: The undersigned consents to the search and seizure of any Device in the undersigned's possession by the District, the District's authorized representative, a System Administrator, or any Peace Officer at any time of the day or night and by any means. This consent is unlimited and shall apply to any Device that is in the possession of the undersigned, whenever the possession occurs, and regardless of whether the possession is authorized. The undersigned waives any rights that may apply to searches of Devices under SB 178 as set forth in Penal Code sections 1546 through 1546.4.

Student Acknowledgment

I have received, read, understand, and agree to abide by Board Policy 6163.4, this Agreement, and other applicable laws and District policies and regulations governing the use of Devices. I understand that there is no expectation of privacy when using Devices. I hereby release the District and its personnel from any and all claims and damages arising from my use of Devices or from the failure of any technology protection measures employed by the District. I further understand that any violation may result in loss of user privileges, disciplinary action, and/or appropriate legal action.

Name (Please print) _____ Grade: _____

School: _____

Signature: _____ Date: _____

Parent or Legal Guardian Acknowledgment

If the student is under 18 years of age, a parent/guardian must also read and sign the Agreement.

As the parent/guardian of the above-named student, I have read, understand, and agree that my child shall comply with Board Policy 6163.4 and the terms of the Agreement. By signing this Agreement, I give permission for my child to use Devices and/or to access the school's computer network and the Internet. I understand that, despite the District's best efforts, it is impossible for the school to restrict access to all offensive and controversial materials. I agree to release from liability, indemnify, and hold harmless the school, District, and District personnel against all claims, damages, and costs that may result from my child's use of Devices or the failure of any technology protection measures used by the District. Further, I accept full responsibility for supervision of my child's use of his/her access account if and when such access is not in the school setting.

Name: (Please print) _____ Date: _____

Signature: _____