OROVILLE UNION HIGH SCHOOL DISTRICT
ACCEPTABLE USE AGREEMENT
INTERNET / EMAIL and WEB PUBLISHING PERMISSION FORM

Student does not have permission to use e-mail and the internet at school unless this form is signed. Parent/Guardian agrees not to hold the district or any district staff responsible for the failure of any technology protection measures or use mistakes or negligence and shall agree to indemnify and hold harmless the district and district staff for any damages or costs incurred.

Students, faculty, staff and visitors at district schools are expected to use technology and the internet as educational resources. The following procedures and guidelines are used to help ensure appropriate use of the technology and the internet:

Student Technology Use Expectations and Rules of Appropriate Use

Students are responsible for appropriate behavior on the school's computer network just as they are in a classroom or on school grounds. Communications on the network/systems are often public in nature. No assumption of confidentiality is assumed. General school rules for behavior and communications apply. It is expected that users will comply with district standards and the specific rules set forth below. The use of technology is a privilege, not a right, and may be revoked if abused. The user is personally responsible for his/her actions in accessing and utilizing the school's technology resources. Students are not allowed to access, keep, or send anything that they would not want their parents or teachers to see. All of the following rules apply to both district owned and personally owned devices:

1. **Appropriate student use of technology specifically prohibits**:
    a. 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.
    b. 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"
    c. 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
    d. Engaging in any illegal activities on the internet.
    e. Downloading or installing anything including software, shareware, or freeware onto computer drives or disks, unless they have permission from the Network Administrator.
    f. Copying other people's work or intruding into other people's files.
    g. Disclosing personal information, such as name, school, address, and telephone number outside of the school network.
2. Students shall only use electronic mail, chat rooms, and other forms of direct electronic communications for school-related purposes and only as directed by faculty and staff.
3. Students will be held accountable for their actions and for the loss of privileges if the Rules of Appropriate Use are violated.
4. Students shall notify the teacher or OUHSD staff member immediately, if by accident, they encounter materials which violate the boundaries of appropriate use.

Any violation of school policy and rules may result in loss of school-provided access to technology. Additional disciplinary action may be determined in keeping with existing school policies and procedures. When and where applicable, law enforcement agencies may be involved.

Oroville Union High School District (OUHSD) Policy

a. OUHSD uses various security measures that block or filter access to internet sites that are not in accordance with the policy of the district.

b. Security measures may be overridden by an OUHSD staff member for legitimate research purposes. **Students are not allowed to bypass the security measures for any reason**.

c. OUHSD staff may monitor student use of the internet through direct supervision, monitoring software, or other means to ensure enforcement of these policies.

d. Click here to read the complete OUHSD Board Approved Policy regarding Student Use of Technology.

Instruction

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

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 6777; 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

(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
6751-6777 Enhancing Education Through Technology Act, Title II, Part D, especially:
6777 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

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

Adopted: 10/3/01
Amended: 9/19/07, 11/18/09, 9/16/15

Oroville Union High School District
Acceptable Use Agreement and Release of District from Liability (Students)

Your student does not have permission to use any school technology unless this form is signed.

The Oroville Union High School District authorizes students to use technology owned or otherwise provided by the district as necessary for instructional purposes. The use of district technology is a privilege permitted at the district's discretion and is subject to the conditions and restrictions set forth in applicable Board policies, administrative regulations, and this Acceptable Use Agreement. The district reserves the right to suspend access at any time, without notice, for any reason.

The district expects all students to use technology responsibly in order to avoid potential problems and liability. The district may place reasonable restrictions on the sites, material, and/or information that students may access through the system.

Each student who is authorized to use district technology and his/her parent/guardian shall sign this Acceptable Use Agreement as an indication that they have read and understand the agreement.

Definitions

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.

Student Obligations and Responsibilities

Students are expected to use district technology safely, responsibly, and for educational purposes only. The student in whose name district technology is issued is responsible for its proper use at all times. Students shall not share their assigned online services account information, passwords, or other information used for identification and authorization purposes, and shall use the system only under the account to which they have been assigned.

Students are prohibited from using district technology for improper purposes, including, but not limited to, use of district technology to:

1. Access, post, display, or otherwise use material that is discriminatory, libelous, defamatory, obscene, sexually explicit, or disruptive

2. Bully, harass, intimidate, or threaten other students, staff, or other individuals ("cyberbullying")

3. Disclose, use, or disseminate personal identification information (such as name, address, telephone number, Social Security number, or other personal information) of another student, staff member, or other person with the intent to threaten, intimidate, harass, or ridicule that person

4. Infringe on copyright, license, trademark, patent, or other intellectual property rights

5. Intentionally disrupt or harm district technology or other district operations (such as destroying district equipment, placing a virus on district computers, adding or removing a computer program without permission from a teacher or other district personnel, changing settings on shared computers)

6. Install unauthorized software

7. "Hack" into the system to manipulate data of the district or other users

8. Engage in or promote any practice that is unethical or violates any law or Board policy, administrative regulation, or district practice

Privacy

Since the use of district technology is intended for educational purposes, students shall not have any expectation of privacy in any use of district technology.

The district reserves the right to monitor and record all use of district technology, including, but not limited to, access to the Internet or social media, communications sent or received from district technology, or other uses. 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 district technology (such as web searches and emails) cannot be erased or deleted.

All passwords created for or used on any district technology are the sole property of the district. The creation or use of a password by a student on district technology does not create a reasonable expectation of privacy.

Personally Owned Devices

If a student uses a personally owned device to access district technology, he/she shall abide by all applicable Board policies, administrative regulations, and this Acceptable Use Agreement. Any such use of a personally owned device may subject the contents of the device and any communications sent or received on the device to disclosure pursuant to a lawful subpoena or public records request.

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 district technology, he/she shall immediately report such information to the teacher or other district personnel.

Consequences for Violation

Violations of the law, Board policy, or this agreement may result in revocation of a student's access to district technology 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 appropriate.

Student Acknowledgment

I have received, read, understand, and agree to abide by this Acceptable Use Agreement and other applicable laws and district policies and regulations governing the use of district technology. I understand that there is no expectation of privacy when using district technology. I further understand that any violation may result in loss of user privileges, disciplinary action, and/or appropriate legal action.

Name: _____ Grade: _____
(Please print)

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 the terms of the Acceptable Use Agreement. By signing this Agreement, I give permission for my child to use district technology 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 district technology 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: _____ Date: _____
(Please print)

Signature: _____