Calaveras Unified School District
Acceptable Use Policy (AUP) for District Computer Systems
Information for all Staff and Students

The District's Acceptable Use Policy ("AUP") is to prevent unauthorized access and other unlawful activities by users online, prevent unauthorized disclosure of or access to sensitive information, and to comply with the Children's Internet Protection Act ("CIPA"). As used in this policy, "user" includes anyone using the computers, Internet, email, chat rooms and other forms of direct electronic communications or equipment provided by the District (the "network"). Only current students or employees are authorized to use the network.

The District will use technology protection measures to block or filter, to the extent practicable, access of visual depictions that are *obscene, pornographic, and harmful to minors* over the network. The District reserves the right to monitor users' online activities and to access, review, copy, and store or delete any electronic communication or files and disclose them to others as it deems necessary. Users should have no expectation of privacy regarding their use of District property, network and/or Internet access or files, including email.

Acceptable Uses of the District Computer Network or the Internet

 Each year the District must verify that a student has signed the acknowledgment page of this policy in order for the student to use the computer network and to have Internet Access. Each school site must keep this page on file. A student who is under 18 must have a parent or guardian sign this page and schools must keep it on file. Once signed the permission/acknowledgement page remains in effect until revoked by the parent, or the student loses the privilege of using the District's network due to violation of this policy or is no longer a CUSD student. Employees and other users are required to follow this policy. Even without signature, all users must follow this policy and report any misuse of the network or Internet to a teacher, supervisor or other appropriate District personnel. Access is provided primarily for education and District business. Staff may use the Internet, for incidental personal use during duty-free time. By using the network, users have agreed to this policy. If a user is uncertain about whether a particular use is acceptable or appropriate, the user should consult a teacher, supervisor or other appropriate District personnel.

In addition, each year a student must pass a basic Netiquette class verified by the school site at which the student attends. Netiquette, or network etiquette, is the contemporary term for the proper way to communicate and interact with each other using email over the Internet. Netiquette training will include but is not limited to:
- Becoming familiar with CUSD's AUP
- Common courtesy in written communication
- Asking permission to forward attachments or emails

Unacceptable Uses of the Computer Network or Internet

These are examples of inappropriate activity on the District web site, but the District reserves the right to take immediate action regarding activities (1) that create security and/or safety issues for the District, students, employees, schools, network or computer resources, or (2) that expend District resources on content the District in its sole discretion determines lacks legitimate educational content/purpose, or (3) other activities as determined by District as inappropriate.

Violating any state or federal law or municipal ordinance, such as: Accessing or transmitting pornography of any kind, obscene depictions, harmful materials, materials that encourage others to violate the law, confidential information or copyrighted materials;
- **Criminal activities** that can be punished under law;
- **Selling or purchasing** illegal items or substances;
- **Obtaining and**/or using anonymous email sites; spamming; spreading viruses;
- **Causing harm** to others or damage to their property, such as:
  1. Using profane, abusive, or impolite language; threatening, harassing, or making damaging or false statements about others or accessing, transmitting, or downloading offensive, harassing, or disparaging materials;
  2. Deleting, copying, modifying, or forging other users' names, emails, files, or data; disguising one's identity, impersonating other users, or sending anonymous email;
  3. Damaging computer equipment, files, data or the network in any way, including intentionally accessing, transmitting or downloading computer viruses or other harmful files or programs, or disrupting any computer system performance;
  4. Using any District computer to pursue "hacking," internal or external to the District, or attempting to access information protected by privacy laws; or
  5. Accessing, transmitting or downloading large files, including "chain letters" or any type of "pyramid schemes".
- **Engaging in uses that** jeopardize access or lead to unauthorized access into others' accounts or other computer networks, such as:
  1. Using another's account password(s) or identifier(s);
  2. Interfering with other users' ability to access their account(s); or
  3. Disclosing anyone's password to others or allowing them to use another's account(s).

- **Using the network** or Internet for Commercial purposes:
    1. Using the Internet for personal advertising, promotion, or financial gain; or
    2. Conducting for-profit business activities and/or engaging in non-government related fundraising or public relations activities such as solicitation for religious purposes, lobbying for personal political purposes.

Student Internet Safety

1. Students under the age of eighteen should only access District accounts outside of school if a parent or legal guardian supervises their usage at all times. The student's parent or guardian is responsible for monitoring the minor's use;
2. Students shall not reveal on the Internet personal information about themselves or other persons. For example, students should not reveal their name, home address, telephone number, or display photographs of themselves or others;
3. Students shall not meet in person anyone they have met only on the Internet; and
4. Students must abide by all laws, this Acceptable Use Policy and all District security policies.

What Cyberbullying is and NOT allowed

- **Flaming.** Online fights using electronic messages with angry or vulgar language.
- **Harassment.** Repeatedly sending nasty, mean, an insulting messages.
- **Denigration.** "Dissing" someone online. Sending or posting gossip or rumors about a person to damage his or her reputation or friendships.
- **Impersonation.** Pretending to be someone else and sending or posting material to get that person in trouble or damage their reputation.
- **Outing.** Sharing someone's secrets or embarrassing information or images online.
- **Trickery.** Tricking someone into revealing secrets or embarrassing information and then sharing it online.
- **Exclusion.** Intentionally and cruelly excluding someone.
- **Cyberstalking.** Repeated, intense harassment and denigration that includes threats or creates significant fear.

Penalties for Improper Use

The use of a District account is a privilege, not a right, and misuse will result in the restriction or cancellation of the account. Misuse may also lead to disciplinary and/or legal action for both students and employees, including suspension, expulsion, dismissal from District employment, or criminal prosecution by government authorities. The District will attempt to tailor any disciplinary action to the specific issues related to each violation.

- **Software:** CUSD laptops are provided with district standard software (e.g., operating system, Microsoft Office Professional, site licensed software) and access to CUSD networks only for work-related projects. All installations of software MUST go through the tech department, with a copy of the license agreement.
- **Privacy:** System users should have no expectation of privacy in the contents of files and records maintained on district equipment. Do not use equipment for personal use.
- **Negligence:** Staff members may be held personally responsible for abuse or negligence. Staff members are to report any instance of theft or vandalism to the immediate supervisor within twenty-four (24) hours.
- **Network Security:** The district uses network management technology to protect equipment and systems from viruses and related security violations. Users may not use *types of knowledge* to bypass the district filter and/or firewall.
- **Technical Assistance:** The District cannot provide technical assistance and maintenance for applications or hardware not identified in the standard CUSD image for laptops.
- **Data Security:** The district provides secured, encrypted access to student records across the Internet. Some of the data stored in our student, fiscal, and employee information systems are sensitive. Personal data that could be used in identity theft such as social security numbers or addresses, whether for students or adults, *may never be stored on computers*.

Disclaimer

Calaveras Unified School District
Acceptable Use Policy (AUP) for District Computer Systems
Information for all Staff and Students

The District makes no guarantees about the quality of the services provided and is not responsible for any claims, losses, damages, costs, or other obligations arising from use of the network or accounts. Any additional charges a user accrues due to the use of the District's network are to be borne by the user. The District also denies any responsibility for the accuracy or quality of the information obtained through user access. Any statement, accessible on the computer network or the Internet, is understood to be the author's individual point of view and not that of the District, its affiliates, or employees.

Student Information

I have read, understand, and agree to abide by the provisions of the Acceptable Use Policy of the Calaveras Unified School District.		
Site Location:		
	Student	**Parent**
Date:		
Print *name clearly*		
Signature:		

Employee Information

I have read, understand, and agree to abide by the provisions of the Acceptable Use Policy of the Calaveras Unified School District.	
Site Location:	
Date:	
Print *name clearly*	
Signature:	

Please return this form to the school or office where it will be kept on file.
It is required for all staff and students that will be using a computer network and/or Internet access.

For Internal Use ONLY:

User Job Description/Title:	
School Site/room#/Job Share w/who:	
Personnel Signature/Date	
Technology Signature:	
Date:	
Please send this form to the tech department.	