Yuba City Unified School District

Internet Safety Policy

The Yuba City Unified School District strongly believes in the educational value of electronic services and recognizes their potential to support the curriculum and student learning by facilitating resource sharing, innovation, and communication.

1. Access to Inappropriate Material

a. The District employs an Internet filtering system designed to prevent students and adults from accessing obscene, pornographic, and other materials harmful to minors, as those terms are defined in the Children's Internet Protection Act ("CIPA").

b. These safeguards may be disabled for adults only for bona fide research or other lawful purpose.

2. District Monitoring and Education

a. The District will monitor the online activities of minors to prevent minors' access to obscene, pornographic, and other materials harmful to minors, as those terms are defined in CIPA.

b. To the extent possible, it is the duty of all District teachers and staff to educate minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.

Acceptable Use Agreement

All users of the District's networking services must sign this Agreement acknowledging and agreeing to the following standards and requirements.

Parents must closely review this Agreement. Both parents and their children are ultimately responsible for complying with its terms. Please refer to the Internet section of the District's Student Discipline Handbook for additional information. (References are not an exhaustive list).

1. Personal Safety

a. Students may not disseminate or distribute personal contact information about themselves or other people without the permission of their parents, teacher, and any affected third party. Personal contact information includes but is not limited to photos, addresses or telephone numbers. (Safety violation)

b. Students may not meet in person with someone they have met online without their parent's approval. (Safety violation)

c. Students will promptly disclose to their teacher or other school employee any message they receive that is inappropriate. Inappropriate messages are those that are obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful. (Safety violation)

2. Illegal Activities

a. Students and staff may not attempt to gain unauthorized access ("hacking") to the District's network resources or to any other computer system to go beyond their authorized access.

This includes attempting to log-in through another person's account or access another person's files. These actions are illegal, even if only for the purposes of "browsing." (Theft)

b. Students and staff may not make deliberate attempts to disrupt the computer system or destroy data by spreading computer viruses or by any other means. These actions are illegal. (Vandalism)

c. Students and staff may not use the District network to engage in any other illegal act, such as arranging for a drug sale, engaging in criminal gang activity, or threatening the safety of a person. (Drug and safety violation)

d. Students and staff may not read, move, rename, edit, delete, or in any way alter the files that have been created or organized by others without express permission. (Vandalism)

e. Students and staff may not install software on any District computers or on the District network without the direct approval and supervision of District staff. (Vandalism)

f. Students and staff may not alter hardware or software setups on any District computer resources. (Vandalism)

3. <u>Security</u>

a. Students and staff are responsible for their individual accounts and should take all reasonable precautions to prevent others from gaining access. (Safety violation)

b. Students and staff must immediately notify a teacher, campus administrator, or other appropriate authority if they identify a possible security problem with the network or peripheral computers. Students and staff may not go looking for these security problems, because this may be construed as an attempt to gain improper or illegal access in violation of this Agreement. (Safety violation/theft)

c. Students and staff must take all precautions to avoid the spread of computer viruses. (Vandalism)

d. Students and staff may not attach any computer equipment, mobile devices (including smartphones and/or tablets) or other peripherals to the District network or its infrastructure without District approval. "Computer equipment or peripherals" does not include data storage devices such as USB drives, flash drives, floppy disks, CDs, or DVDs. (Safety)

4. <u>Inappropriate Language</u>

a. Students and staff may not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language. (Derogatory statements/sexual harassment)

b. Restrictions against inappropriate language apply to public messages, private messages, emails, and material created for assignments or to be disseminated or distributed on web pages. (Derogatory statements/disruption of education)

c. Students and staff may not engage in personal attacks, including prejudicial or discriminatory attacks through their use of District network services or technology. (Derogatory statements/disruption of education)

d. Students and staff may not harass other people through their use of the District's network systems or technology. Harassment is persistently acting in a manner that distresses or annoys another person. If students or staff are told by a person to stop sending them such messages, I will stop. (Disrespecting others' rights/disruption of education)

e. Students and staff may not knowingly or recklessly disseminate or distribute false or defamatory information about a person or organization through their use of the District's network or technology resources. (Derogatory statements/disruption of education)

5. Respect for Privacy

a. Students and staff may not redistribute messages that were sent to them privately without permission of the person who sent them the message. (Disrespecting others' rights)

b. Students and staff may not disseminate or distribute private information about another person through the use of the District's network or technology resources. (Disrespecting others' rights)

6. Respecting Resource Limits

a. Students must use the technology and network only for educational purposes. (Disruption of education)

b. Staff must use the District's network and technology primarily for work-related purposes. Staff may engage in minimal personal use of the technology and network, provided that such use does not interfere with their employment obligations to the District and/or otherwise breach this Agreement or any applicable collective bargaining agreement.

c. Students and staff may not disseminate or distribute chain letters or engage in "spamming." Spamming is sending an annoying or unnecessary message to a large number of people. (Disruption of education)

d. Students and staff may not download or use games, pictures, video, music, instant messaging, e-mail, or file sharing applications, programs, executables, or similar materials unless authorization is first obtained from the District, it is legal for to possess such files, and it is in support of a classroom assignment or employment duties to the District. (Disruption of education)

e. Students understand that District personnel may monitor and access any equipment connected to the District's network resources and my computer activity. The District personnel may delete any files, program and/or media that are not for a classroom assignment. (Security)

7. Plagiarism and Copyright Infringement

a. Students may not plagiarize works found on the Internet or on the computers at my school. Plagiarism is taking the ideas or writings of others and presenting them as if they were my own. (Theft)

b. Students and staff may not engage in copyright infringement. Copyright infringement occurs when students or staff inappropriately reproduce a work that is protected by a copyright. If a work contains language that specifies or limits the way(s) in which a work may be used, students and staff may use the work only as specified by the copyright holder. If students or staff are unsure whether a particular work may be used, permission must first be requested from the copyright holder. (Theft)

8. Inappropriate Access to Material

a. Students and staff may not use District network resources to access or store material that is profane, obscene (pornography), that advocates illegal acts, or that advocates violence and/or discrimination toward other people. (Disruption of education/safety violation)

b. Should students and/or staff mistakenly access inappropriate material, they must immediately tell their teacher, appropriate administrator, or supervisor, and will not attempt to access the inappropriate information again. (Failure to comply with directives)

c. Parents will instruct their student(s) as to additional material that they believe is inappropriate for their student to access. Students agree not to access any material that their parents have informed them is inappropriate. (Respect for others violation)

d. Students and staff understand that Internet access is provided for support of classroom assignments and/or employment duties to the District, and agree that they will not attempt to surf anonymously or modify the computer in any way that would allow access to inappropriate websites, programs or files that are not authorized for use. (Disruption of education).

9. Network Use and Access While Off-Campus and/or During Non-Working Hours

a. The provisions of this Agreement govern access to, and the use of, District networking and technology resources for all students and staff while off campus or during non-working hours. Students and staff agree to abide by the terms of this Agreement whenever they use or access District networking and technology resources, regardless of time or location.

10. Use of District-issued hardware

a. From time to time the District may issue hardware to District students and staff for educational or employment-related purposes. Students and staff agree that their use of District-issued hardware will be limited to that necessary to the educational or employment-related purpose(s) for which it was issued.

b. Students and staff agree not to download, install, or access any program, website, file, document, and/or other electronic media except that which is used in furtherance of that educational or employment-related purpose. Students and staff also agree not to delete, modify, or otherwise tamper with any programs, files, documents, and/or other electronic media existing on District-issued hardware at the time it is provided to the student or staff member.

c. Students and staff agree not to disseminate, disclose, or otherwise make use of any confidential, private, or sensitive information they gain access to through or as a result of their use of any District-issued hardware.

d. Students and staff agree to return any District-issued hardware on demand from the District, or immediate at the conclusion of the purpose(s) for which it was issued. Students and staff agree to return any District-issued hardware in the same physical condition, and with the same, programs, files, documents, and/or electronic media with which the hardware was provided.

11. Discipline

a. Failure by students or staff to abide by the terms of this Agreement is grounds for disciplinary action, up to and including expulsion (students) and termination of employment (staff).

My name and signature below represents that I have received, read, and fully understand the Internet Safety Policy and my responsibilities, as defined in the Acceptable Use Agreement above, when using District technological resources

Parents and guardians of children under the age of 18, must also sign below, indicating that they have received, read, and fully understand the Internet Safety Policy and the responsibilities of their student when using District technological resources. The signature of a parent or guardian below acknowledges and accepts full responsibility for their student's compliance with the terms herein, and hereby give their permission for their student to use the District network and Internet services.

_____ _____
Parent or Guardian Printed Name (if student under 18) Date

_____ _____
Parent or Guardian Signature (if student under 18) Date

_____ _____
Student Printed Name Date

_____ _____
Student Signature Date

_____
Student Permanent ID#

_____ _____
Staff Member Printed Name Date

_____ _____
Staff Member Signature Date