ETIWANDA SCHOOL DISTRICT
ACCEPTABLE USE
RULES AND REGULATIONS

We are pleased that electronic information services (including Internet access) are available to students, teachers, and staff. We believe in the educational value of such electronic services and recognize their potential to support curriculum and student learning. Our goal in providing this service is to promote educational excellence by facilitating resource sharing, innovation, and communication.

Acceptable Use of Electronic Information Resources

The Board recognizes the educational value of electronic information resources; however, the protection of students and staff from inappropriate electronic information is of paramount concern. All Internet users must be aware that the inappropriate use of electronic information resources can be a violation of local, state and federal laws. Violations by students can lead to disciplinary action including suspension, expulsion and/or criminal prosecution when appropriate. Violations by employees can lead to disciplinary action, up to and including dismissal, and/or criminal prosecution when appropriate.

In the Etiwanda School District the acceptable use of electronic information resources shall be for educational uses directly related to the established curriculum. **Students and employees may access the electronic information services only after they have completed and have on file the Acceptable Use Agreement appropriately signed.**

Computer files and communication over electronic networks, including email, are not private and students and employees do not have a right to privacy in such information. To ensure proper use of District technology, designated administrators may monitor or audit the District's technological resources, including but not limited to network transmissions, files, and email at any time for any reason without advance notice or consent. The District also reserves the right to delete, without notice, from its network system any email messages or any material from District web pages and servers, which it deems inappropriate as defined by these *Acceptable Use Rules and Regulations* or other school behavioral guidelines. The District has the right to restrict or terminate computer, Internet, email and District network access at any time for any reason.

Electronic communication or other use of District technology may be subject to disclosure under the California Public Records Act. (*See* California Government Code section 6252.)

The superintendent or his/her designee will establish appropriate board policies and administrative regulations (BP 6163.4 & AR 6163.4) to implement the policy.

User Obligations and Responsibilities.

1. **ACCEPTABLE USE** The use of my assigned account or accounts must be in support of education and research. I am personally responsible for this provision at all times when using electronic information services. The District reserves the right to monitor all activity for improper use.
   a. Use of other organizations' electronic resources must comply with rules appropriate to that network.
   b. Transmission or possession of material that is threatening, obscene, disruptive, sexually explicit, protected by trade secret, or that could be construed as harassment or disparagement of others based on their race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs is prohibited.
   c. Use of electronic resources for commercial (i.e. "for-profit") activities is not acceptable.
   d. Use of District electronic resources for political or promotional activities by employees or students urging the support or defeat of any ballot measure or candidate including but not limited to any candidate for election to the governing board of the District is also prohibited. (Education Code section 7054.)
   e. Unauthorized access to other individual data, data systems, resources, entities, or governmental agencies is prohibited.
   f. Use of the system to encourage the use of drugs, alcohol, or tobacco, or promotion of unethical practices or any activity prohibited by law or District policy is prohibited.
   g. Fraudulent or personal use of the District electronic resources is strictly prohibited.
   h. Placement of copyrighted material on District electronic resources without the author's written permission or license is prohibited. Users downloading, possessing or using copyrighted material assume full responsibility for copyright violations and unauthorized use.
   i. Damaging or modifying computers, computer systems, computer networks, or unauthorized alterations to network infrastructure, operating systems, hardware or software is prohibited.
   j. Accessing or modifying another user's account or data is prohibited.
   k. District hardware or software may not be removed from school or District premises without written permission.
   l. Equipment and software not owned by the District is the responsibility of the owner.
   m. Student owned electronic devices shall not be connected to the District network without prior principal approval.
   n. No students or employees shall load programs on district devices nor shall they download programs from the Internet without written approval from the District Technology Department. Please see the Acceptable Student Use of Personally Owned Devices section in AR 6163.4 or Employee Use of Technology in AR 4540.for further information.
   o. In order to reduce network traffic, users may not employ unauthorized audio or video streaming, real-time messaging features such as talk/chat/Internet relay, etc.
   p. Use of electronic information services for plagiarism is prohibited.
   q. Employees shall not transmit confidential or identifying information about students, parents, or employees without written authorization of the Superintendent or designee. For purposes of this provision, confidential information includes, but is not limited to, the addresses, telephone numbers, last names, educational or personal facts or records of students or personal data about employees or other persons. Emails may not be transmitted to students or parents of students on matters unrelated to said student's education.
   r. False or unverified statements about others may be defamatory and may subject the publisher (speaker or writer) of the statements to civil liability. The District's technology resources may not be used to defame or disparage others.

   I am aware that the inappropriate use of electronic information resources can be a violation of local, state and federal laws and that I can be prosecuted for violating those laws.

2. **SOCIAL NETWORKING** Please see BP 1114 for more information on social networking.

3. **CLOUD COMPUTING** While the Etiwanda School District does not prohibit the use of popular cloud-based storage services such as Google Drive, Dropbox and Skydrive, it is important to note that such services are inherently less secure than traditional storage on

district servers and flash drives. Passwords and logins can be saved to the cloud without your explicit consent. Therefore it is required that all staff members observe the following when using cloud storage:

CLOUD COMPUTING (CONTINUED)

1) Do not use cloud storage services to store sensitive, confidential or personably identifiable information. Please remember that most student information is subject to the Family Educational Rights and Privacy Act (FERPA) and should therefore not be stored in the cloud.

2) Do not use cloud storage services to store Class 1, 2 or 3 District Records. Please see AR 3580 for more information on District Records.

4. **FILTERING** The Etiwanda School District utilizes content filtering technology that restricts or prevents access to Internet content in accordance with the requirements of CIPA (Child Internet Protection Act) and the guidelines established to support the educational goals of the district. At a minimum, content filtering shall prevent access to obscene, profane, sexually oriented, harmful, or illegal content. While district filtering technology is state of the art and diligently monitored, no filtering technology can guarantee that staff and students will be prevented from accessing all inappropriate content on the Internet; therefore it is crucial that staff and students engage in appropriate online behavior and follow the rules and regulations in this document.

5. **BULLYING / CYBER-BULLYING** The Board strives to provide a safe, positive learning climate for students in the schools. Therefore, it shall be the policy of the Etiwanda School District to maintain an educational environment in which bullying and cyber-bullying in any form are not tolerated.

All forms of bullying and cyber-bullying by school district staff, students, or third parties are hereby prohibited by the district. Anyone who engages in bullying or cyber-bullying in violation of this Policy shall be subject to appropriate discipline. In addition, any communication that disrupts or prevents a safe and positive educational or working environment may also be considered Cyber-Bullying. Staff, students, or third parties will refrain from using personal communication devices or district property to harass or stalk another individual.

Students who have been bullied or cyber-bullied shall promptly report such incidents to an appropriate staff member.

Complaints of bullying or cyber-bullying shall be investigated promptly, and corrective action shall be taken when a complaint is verified. Neither reprisals nor retaliation shall occur as a result of the submission of a complaint.

The School District shall annually inform students that bullying or cyber-bullying of students will not be tolerated.

Please see BP 5131 for more information on bullying / cyber-bullying.

6. PRIVATELY OWNED ELECTRONIC EQUIPMENT When approved by the school or district site, privately owned electronic equipment such as tablets, eReaders, iPods, iPads, Nooks, Kindles, iPhones, Samsung, etc. will be permitted to use the wireless guest network for legitimate school and district work / communications. Students and employees must follow the rules and guidance of the school or district site for any use or prohibition of use of such devices. Please see the Acceptable Student Use of Personally Owned Devices section in AR 6163.4 or Employee Use of Technology in AR 4540.for further information.

7. **DISTRICT ELECTRONIC EQUIPMENT** Such as desktop computers and their peripherals, laptops, mobile devices, etc., must be treated in a professional manner using good judgment as to prevent physical damage and software-related issues. Physical damage is defined as anything outside of normal wear and tear. This includes defacement: Equipment returned with stickers, crayon marks or other such “personalization” is not acceptable. When any employee returns electronic equipment to the district, they are to return the equipment in the same condition as received. Good judgment in preventing software-related issues includes using the equipment judiciously and avoiding activities likely to infect the equipment with malware, worms, viruses, etc. Additionally, employees are not permitted to install software on district electronic equipment which has not been pre-approved by the district. Any employee found to have installed non-district approved software or who irresponsibly uses the equipment in a manner which results in operating system or software corruption will receive a warning. Subsequent occurrences will result in the removal of privileges to install/modify software on the equipment.

For more information, refer to the Electronic Resource Guidelines document http://www.etiwanda.org/district/empforms/ElecResGuide.pdf