CHILDREN'S INTERNET PROTECTION ACT
INTERNET SAFETY POLICY

The District maintains computers at school sites and other facilities within the District to provide access to online technology systems such as the Internet, the World Wide Web, electronic mail, chat rooms, and other forms of direct electronic communications. The School Board intends that technological resources provided by the District be used in a safe, responsible, and proper manner in support of the instructional program and for the advancement of student learning. The School Board also recognizes that some of the material and information available through these technology systems are inappropriate and not suitable in an educational setting. In an effort to minimize or eliminate access through District computers to material or information that is inappropriate and unsuitable, the School Board adopts this policy pursuant to the requirements of the Children's Internet Protection Act ("CIPA").

In order to be eligible for certain federal funds, and in order to qualify for universal service benefits, the School District must comply with the following:

School District computers shall have a technology protection measure that protects against Internet access by both adults and minors to visual depictions that are obscene, child pornography, or, with respect to use of the computers by minors, harmful to minors.

All online activities of minors shall be monitored by the teacher and teacher's assistants responsible for the classroom in which the computers are located.

1. Minors shall not be permitted to access inappropriate matter on the Internet and World Wide Web.

2. Teachers and teacher's assistants shall be responsible for the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communication.

3. Teachers and teacher's assistants shall not permit unauthorized access, including so-called "hacking," and other unlawful activities by minors online.

4. Teachers and teacher's assistants shall not permit unauthorized disclosure, use, and dissemination of personal information regarding minors.

5. In addition, students may not be given access to Internet and on-line sites that contain harmful matter as defined in subdivision (a) of Section 313 the Penal Code. EC 51870.5

CHILDREN'S INTERNET PROTECTION ACT
INTERNET SAFETY POLICY

The Superintendent or designee shall notify students and parents/guardians about authorized uses of District computers, user obligations and responsibilities, and consequences for unauthorized use and/or unlawful activities in accordance with District regulations and the District's Acceptable Use Agreement. Before a student is authorized to use the District's technological resources, the student and his/her parent/guardian shall sign and return the Acceptable Use Agreement specifying user obligations and responsibilities. In that agreement, the student and his/her parent/guardian shall agree not to hold the District or any District staff responsible for the failure of any technology protection measures, violations of copyright restrictions, or user mistakes or negligence. They shall also agree to indemnify and hold harmless the District and District personnel for any damages or costs incurred.

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 personal information online, misrepresentation by online predators, how to report inappropriate or offensive content or threats, behaviors that constitute cyber-bullying, and how to respond when subjected to cyber-bullying.

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. Staff shall supervise students while they are using online services and may have teacher aides, student aides, and volunteers assist in this supervision. District staff is prohibited from consenting to the release of student information unless written permission from parent/guardian has been received.

Student use of District computers to access social networking sites is prohibited with the exception of District approved and provided social networking sites. To the extent possible, the Superintendent or designee shall block access to such sites on District computers with Internet access.

Regarding the use of a technology protection measure to minimize or eliminate access to material or information that is inappropriate and/or harmful to students, the School Board recognizes that such technology protection measures may not be error-free or without defect. Therefore, District procedures shall also address the manner in which the District will identify, investigate, and correct, if necessary, such errors or defects.

The Superintendent or designee shall regularly review and update this policy and other relevant procedures to enhance the safety and security of students using the District's

technological resources and to help ensure that the District adapts to changing technologies and circumstances.

Penal Code Section 313 defines harmful matter as follows:

313. As used in this chapter:

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

(1) When it appears from the nature of the matter or the circumstances of its dissemination, distribution or exhibition that it is designed for clearly defined deviant sexual groups, the appeal of the matter shall be judged with reference to its intended recipient group.

(2) In prosecutions under this chapter, where circumstances of production, presentation, sale, dissemination, distribution, or publicity indicate that matter is being commercially exploited by the defendant for the sake of its prurient appeal, that evidence is probative with respect to the nature of the matter and can justify the conclusion that the matter lacks serious literary, artistic, political, or scientific value for minors.

(b) "Matter" means any book, magazine, newspaper, video recording, or other printed or written material or any picture, drawing, photograph, motion picture, or other pictorial representation or any statue or other figure, or any recording, transcription, or mechanical, chemical, or electrical reproduction or any other articles, equipment, machines, or materials. "Matter" also includes live or recorded telephone messages when transmitted, disseminated, or distributed as part of a commercial transaction."

As used in this policy, the terms "minor," "obscene," "child pornography," "harmful to minors" and technology protection measure," are defined in the Children's Internet Protection Act § 1721 (c).

Students violating this policy may be subject to discipline, including denial of computer use privileges, and suspension and/or expulsion pursuant to Education Code Section 48900 (k), and the Board's Suspension and Expulsion Policy.

CHILDREN'S INTERNET PROTECTION ACT
INTERNET SAFETY POLICY

Employees violating this policy may be subject to discipline, including suspension and/or dismissal pursuant to Board Policy and the California Education Code.

Legal Reference:

Re: 47 U.S.C. §254 (h); EC 51870.5; PC 313;
http://www.fcc.gov/Bureaus/Common Carrier/Orders/2001/fcc01120.doc
http://www.access.gpo.gov/su_docs/aces/aces140.html
http://www.leginfo.ca.gov/calaw.html

UNITED STATES CODE, TITLE 15
6501-6506 Children's Online Privacy Act

UNITED STATES CODE, TITLE 20
7001 Children's Internet Protection Act
6751-6777 Enhancing Education through Technology Act, Title II, Part D, especially: 6777 Internet safety
6801 et seq. Elementary and Secondary Education Act of 1965, as amended

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,
especially: 54.520(c)(1)(i), 54.520(c)(2)(i) Protecting Children in the 21st Century Act
Children's Internet Protection Act of 2000 (H.R. 4577, PL. 106-554)
Communications Act of 1934, as amended (47 U.S.C. 254[h], [I]
Elementary and Secondary Education Act of 1965, as amended 920 U.S.C.
6801 et. Seq., Part F

EDUCATION CODE
51006 Computer education and resources
51007 Programs to strengthen technological skills
51870-51874 Education technology
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

Policy **LUCERNE ELEMENTARY SCHOOL DISRICT**
adopted: June 12, 2002 Lucerne, California
revised: June13, 2012