MEMORANDUM

TO: SCHOOL DISTRICT BOARD OF TRUSTEES

FROM: ELMER D. PORTER

SUBJECT: CIPA COMPLIANCE

DATE: 11/21/2001

CC: ROBERT AUMAUGHER, SUPERINTENDENT

Board Members,

Attached are documents, which outline the Children's Internet Protection Act (CIPA) that was adopted by the Federal Communications Commission (FCC) in March 2001. All schools and public libraries that wish to receive E-Rate funding will have to certify CIPA compliance within E-Rate funding year 4. CIPA compliance also is required for schools receiving Title III funds from the Elementary and Secondary Education Act. Eureka County School District (ECSD) has applied for and expects to receive year 4 E-Rate funding after January 1, 2002. In accordance with the rules regarding CIPA compliance outlined within the E-Rate guidelines I have included some background information and mention steps the District must take to become CIPA compliant.

Background of CIPA & E-Rate

The Children's Internet Protection Act (CIPA) was signed into law on December 21, 2000. Under CIPA, no school or library may receive E-Rate discounts unless it certifies that it is enforcing a policy of Internet safety that includes the use of filtering or blocking technology. This Internet Safety Policy must protect against access, through computers with Internet Access, to visual depictions that are obscene, child pornography, or harmful to minors. The school or library must also certify that it is enforcing the operation of such filtering or blocking technology during any use of such computers by minors. The law is effective for funding year 4 (07/01/01-06/30/2002) and for all future years.

Compliance with the requirements of CIPA

1. *Technology Protection Measure*

A Technology Protection Measure is a specific technology that blocks or filters Internet access. It must protect against access by adults and minors to visual depictions that are obscene, child pornography, or harmful to minors. It may be disabled for adults engaged in bona fide research or other lawful purposes. For schools, the policy must also include monitoring the online activities of minors.

Elmer D. Porter, Technology Director/Systems Engineer
Eureka County School District
1 McCoy Street, Eureka, Nevada 89316

Voice: (775) 237-5373, Fax: (775) 237-5014
E-mail: eporter@eureka.k12.nv.us
Web Site: http://www.eureka.k12.nv.us

2. Internet Safety Policy

The Internet Safety Policy must address the following issues:

- access by minors to appropriate matter on the Internet and World Wide Web;
- the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;
- unauthorized access, including so-called "hacking," and other unlawful activities by minors online;
- unauthorized disclosure, use, and dissemination of personal information regarding minors; and
- measures designed to restrict minors' access to materials harmful to minors.

3. Public Notice and Hearing

The authority with the responsibility for administration of the school or library must provide reasonable public notice and hold at least one public hearing to address a proposed Technology Protection Measure and Internet Safety Policy.

For your reading enjoyment, I have included the FCC Docket outlining CIPA and it's requirements. Also included, is the ECSD Acceptable Use Policy (AUP), which, currently is used throughout the District.

If you have any questions, please let me know.

Elmer D. Porter, Technology Director

Additions to ECSD CIPA Policy Requirements for Compliance April, 2012

Additional information added to CIPA policy April, 2012

Protecting Children in the 21st Century Act

The majority of young people make positive choices online, effectively respond to the negative situations that do occur, and are not overly distressed by online situations. They may make mistakes that could be prevented through better education. A minority of young people face greater risks that must be addressed through effective prevention and intervention.

The Protecting Children in the 21st Century Act added a provision to the Children's Internet Protection Act (CIPA) requiring that schools receiving E-Rate and other technology funds provide instruction in Internet safety.1 On August 11, 2011, the Federal Communications Commission issued regulations on this act. Under these regulations, districts must have an Internet safety policy that meets the following requirement: This Internet safety policy must also include monitoring the online activities of minors and must provide for educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.

The primary difference between CIPA and the Protecting Children Act is the latter requires schools to actually educate minors related to the online behaviors referenced in the act. Schools must have an updated internet safety policy that addresses "Educating minors" requirements by July 2012.

To comply with the additional provisions to the CIPA act as outlined in the Protecting Children in the 21st Century Act, ECSD will provide instruction to students and incorporate the guidelines set forth in the act.

5th, 6th, 7th, 8th grade curriculum integration

1. Effective Internet Safety Education

2. Cyber Savvy Strategy

    - Keep Students Safe. They understand the risks-and they know how to avoid getting into risky situations, to detect whether they are at risk, and to effectively respond.

    - Present a Positive Image. They present themselves online as someone who make positive choices.

- Respect Others. They respect the rights, privacy, and property of others and treat others with civility.

- Take Responsibility for the Well-being of Others. They help others and report serious concerns to a responsible adult.

3. Instructional Components

Incorporate these three key components into instruction:

- Reinforce Positive Norms. Universal education must promote the positive norms and effective practices held by the majority of the students. This can be accomplished through student-led constructive instruction, use of older students to teach younger students, and messaging ground in the insight into positive norms and practices derived through local surveys.

- Strengthen Effective Skills. Constructive instruction can also help students gain skills through sharing of effective practices and strategies. Effective skills include problem-solving and decision-making. Students must also recognize possible negative influences related to the use of technologies, as well as the influences for making positive choices.

- Encourage Helpful Allies. As helpful allies, young people can provide support to a peer who is at risk or being harmed, challenge irresponsible or hurtful behavior, and report unresolved or serious concerns. Increase skills in responding and emphasize the positive perspective of helpful allies.

4. Key School Action Steps

Implement these key actions steps:

- Establish a Multidisciplinary Coordinating Committee. Include educational technology specialists, school librarians, and health teachers–and the school resource officer if this person will be providing instruction. Collaborative involvement of these professionals is essential.

- Ensure Professional Development. All members of this team require an understanding of the issues and effective instructional approaches that is ground in research insight. A significant amount of disinformation has been disseminated over the last decade about Internet risk. Fear-based messaging and simplistic rules against normative online behavior will not be effective in preventing risk behavior.

(Added April, 2012)