**CIPA requirements for E-Rate funding include the following three items:**

##### 1. Internet Safety Policy

Schools and libraries are required to adopt and enforce an internet safety policy that includes a technology protection measure that protects against access by adults and minors to visual depictions that are obscene, child pornography, or – with respect to use of computers with internet access by minors – harmful to minors. "Minor" is defined as any individual who is under the age of 17.

This internet safety policy must address all of the following:

* Access by minors to inappropriate 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 "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.

Sample located on page 2.

#####

##### 2. Technology Protection Measure

A technology protection measure is a specific technology that blocks or filters Internet access.

The school or library must enforce the operation of the technology protection measure during the use of its computers with Internet access, although an administrator, supervisor, or other person authorized by the authority with responsibility for administration of the school or library may disable the technology protection measure during use by an adult to enable access for bona fide research or other lawful purpose. For example, a library that uses internet filtering software can set up a process for disabling that software upon request of an adult user through use of a sign-in page where an adult user can affirm that he or she intends to use the computer for bona fide research or other lawful purposes.

CIPA uses the federal criminal definitions for obscenity and child pornography. The term "harmful to minors" is defined as "any picture, image, graphic image file, or other visual depiction that – (i) taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; (ii) depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and (iii) taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors."

#####

##### 3. Public Notice and Hearing or Meeting

The authority with responsibility for administration of the school or library must provide reasonable public notice and hold at least one public hearing or meeting to address a proposed technology protection measure and Internet safety policy. For private schools, public notice means notice to their appropriate constituent group.

Additional meetings are not necessary – even if the policy is amended – unless those meetings are required by state or local rules or the policy itself.

**SAMPLE: Internet Safety Policy For <School or Library>**

**Introduction**

It is the policy of <School or Library> to: (a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with the Children’s Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)].

**Definitions**

Key terms are as defined in the Children’s Internet Protection Act.

**Access to Inappropriate Material**

To the extent practical, technology protection measures (or “Internet filters”) shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information.

Specifically, as required by the Children’s Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors.

Subject to staff supervision, technology protection measures may be disabled for adults or, in the case of minors, minimized only for bona fide research or other lawful purposes.

**Inappropriate Network Usage**

To the extent practical, steps shall be taken to promote the safety and security of users of the online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications.

Specifically, as required by the Children’s Internet Protection Act, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called ‘hacking,’ and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

**Education, Supervision and Monitoring**

It shall be the responsibility of all members of the staff to educate, supervise and monitor appropriate usage of the online computer network and access to the Internet in accordance with this policy, the Children’s Internet Protection Act, the Neighborhood Children’s Internet Protection Act, and the Protecting Children in the 21st Century Act.

Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of IT Technician or designated representatives.

The IT Technician or designated representatives will provide age- appropriate training for students who use the Internet facilities. The training provided will be designed to promote the commitment to:

1. The standards and acceptable use of Internet services as set forth in the Internet Safety Policy;
2. Student safety with regard to:
	1. safety on the Internet
	2. appropriate behavior while on online, on social networking Web sites, and in chat rooms; and
	3. cyberbullying awareness and response
3. Compliance with the E-rate requirements of the Children’s Internet Protection Act (“CIPA”).

Following receipt of this training, the student will acknowledge that he/she received the training, understood it, and will follow the provisions of the District's acceptable use policies.

**Adoption**

This Internet Safety Policy was adopted by the Board of <School or Library> at a public meeting, following normal public notice, on <Month, Day, Year>.

CIPA definitions of terms:

**MINOR**. The term “minor” means any individual who has not attained the age of 17 years.

**TECHNOLOGY PROTECTION MEASURE.** The term ``technology protection measure'' means a specific technology that blocks or filters Internet access to visual depictions that are:

**OBSCENE**, as that term is defined in section 1460 of title 18, United States Code; 2.

**CHILD PORNOGRAPHY**, as that term is defined in section 2256 of title 18, United States

Code; or

**HARMFUL TO MINORS.** The term ``harmful to minors'' means any picture, image, graphic image file, or other visual depiction that:

1.Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;

2.Depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and

3.Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

**SEXUAL ACT; SEXUAL CONTACT.** The terms ``sexual act'' and ``sexual contact'' have the meanings given such terms in section 2246 of title 18, United States Code.