

CHILDREN’S INTERNET PROTECTION ACT (CIPA)

Districts must provide individual policies to address CIPA.

Example:

Children’s Internet Protection Act – The District’s CIPA safety policy is incorporated in the Acceptable Use Policy, specifically “In compliance with federal law, the School District shall operate a technology protection measure that blocks or filters Internet access. The technology protection measure shall protect against access by adults and minors to content that is abusive, obscene, profane, sexually explicit, threatening, illegal or pertains to pornography. The School District shall make every effort to restrict access to inappropriate materials and shall monitor the online activities of the end users; however, it is impossible to control all materials on a global network. Therefore, the District shall not be liable for the content or viewing of any materials not prepared by the District.”

The District uses the Fortiguard appliance and Cyber Patrol filtering software provided by the State of South Dakota. Each year the back to school sessions held at each building include a review of the Acceptable Use Policy.

Background

The Children’s Internet Protection Act (CIPA) is a federal law enacted by Congress to address concerns about access to offensive content over the Internet on school and library computers. CIPA imposes certain types of requirements on any school or library that receives funding for Internet access or internal connections from the E-rate program – a program that makes certain communications technology more affordable for eligible schools and libraries. In early 2001, the FCC issued rules implementing CIPA. More recently, Congress enacted additional protections for children using the Internet.

What CIPA Requires

- Schools and libraries subject to CIPA may not receive the discounts offered by the E-rate program unless they certify that they have an Internet safety policy and technology protection measures in place. An Internet safety policy must include technology protection measures to block or filter Internet access to pictures that are: (a) are obscene, (b) child pornography, or (c) harmful to minors (for computers that are accessed by minors).
- Schools and libraries must also certify that, as part of their Internet safety policy, they are educating minors about appropriate online behavior, including cyberbullying awareness and response and interacting with other individuals on social networking sites and in chat rooms.
- Schools subject to CIPA are required to adopt and enforce a policy to monitor online activities of minors.

- Schools and libraries subject to CIPA are required to adopt and implement a policy addressing: (a) access by minors to inappropriate matter on the Internet; (b) the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications; (c) unauthorized access, including so-called “hacking,” and other unlawful activities by minors online; (d) unauthorized disclosure, use, and dissemination of personal information regarding minors; and (e) restricting minors’ access to materials harmful to them.

Schools and libraries are required to certify that they have their safety policies and technology in place before receiving E-rate funding.

- CIPA does not affect E-rate funding for schools and libraries receiving discounts only for telecommunications, such as telephone service.
- An authorized person may disable the blocking or filtering measure during any use by an adult to enable access for bona fide research or other lawful purposes.

CIPA does not require the tracking of Internet use by minors or adults.