

LAKE SUPERIOR SCHOOL DISTRICT #381 INTERNET SAFETY POLICY

Introduction

It is the policy of Lake Superior School District #381 to:

- * Prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications
- * Prevent unauthorized access and other unlawful online activity
- * Prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors
- * Protect students from Cyber-bullying through education and related school discipline policies
- * Comply with the Children's Internet Protection Act (See CIPA information attached)

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 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 Lake Superior School District #381 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.

Supervision and Monitoring

It shall be the responsibility of all members of the Lake Superior School District #381 staff to supervise and monitor usage of the online computer network and access to the Internet in accordance with this policy and the Children's Internet protection Act. Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the Media and Technology Department or designated representatives.

Adoption

The Board of Lake Superior School District #381 has adopted this Internet Safety Policy at a public meeting, following normal public notice, on **November 18th, 2010**

Notes on CIPA (Children’s Internet Protection Act):

CIPA 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.

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 that includes technology protection measures. The protection measures must block or filter Internet access to pictures that are: (a) obscene, (b) child pornography, or (c) harmful to minors (for computers that are accessed by minors). Before adopting this Internet safety policy, schools and libraries must provide reasonable notice and hold at least one public hearing or meeting to address the proposal.
- 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 an Internet safety 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) measures 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.

You can find out more about CIPA or apply for E-rate funding by contacting the Universal Service Administrative Company’s (USAC) Schools and Libraries Division (SLD) at www.sl.universalservice.org. SLD also operates a client service bureau to answer questions at 1-888-203-8100 or via e-mail through the SLD Web site.