

**Children's Internet Protection Act (CIPA) Safety Plan****[Revise and edit as necessary to fit USD goals and include in Handbook]****Goals:**

It is the policy of USD 395 to take the following technology protection or other specified measures in order to better protect our district students from harmful online and electronically transmitted content:

install blocks or Internet filters to the district network in order to limit access by both minors and adults to child pornography and visual depictions or materials that are obscene, inappropriate, or harmful to minors and/or the transmission thereof;

monitor the online activities of students while at school, at school sponsored activities, or while utilizing the district's network, computer system, computers, e-mail system, or electronic devices having access to the Internet;

address issues related to the safety of students when using e-mail, chat rooms, and other electronic communication;

educate students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms as well as on cyberbullying awareness and response;

hinder unauthorized access (hacking) and other unlawful on-line activities by students; and

prevent unauthorized disclosure, use, or dissemination of personal information regarding minors, which shall include, but may not be limited to, personally identifiable information contained in student records; and

comply with the Children's Internet Protection Act.

**Access to Inappropriate Material**

To the extent practicable, technology protection measures or Internet filters shall be used to block or filter the Internet or other forms of electronic devices from accessing child pornography as well as obscene, inappropriate, or harmful material given the age and maturity levels of district students. It is the district's goal to implement and enforce technology protection measures under this plan in such a way as to ensure no minor has access to visual depictions that are child pornography, harmful to minors, or obscene.

Subject to administrative approval, technology protection measures may be minimized only for bonafide research or other lawful purposes that are closely monitored by district staff.

**Inappropriate Network Usage**

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

Specifically, in accordance with CIPA, measures to prevent inappropriate network usage shall include frequent monitoring of the District's network, computer systems, and equipment to detect any unauthorized access to prohibited materials as described earlier in this plan, hacking, and other unlawful activities by students or staff members. Such monitoring shall also strive to detect unauthorized disclosure, use, and dissemination of personally identifiable information regarding students.

### **Education, Supervision and Monitoring**

It shall be the responsibility of all members of the District's staff to educate, supervise, and monitor appropriate usage of online computer network access to the internet in accordance with this policy and CIPA. If, during the course of such monitoring, a student or staff member discovers a violation of this policy, the student or staff member shall make a report as follows:

Students shall report suspected violation of this policy to any classroom teacher.

Staff members shall report suspected violations of this policy to their immediate supervisor when possible.

### **Disciplinary Measures**

The district retains the right to discipline any student, up to and including expulsion, and any employee, up to and including termination, for violation of this policy.

### **Adoption**

This Children's Internet Protection Act Safety Plan was adopted by the Board of USD 395 at a public meeting, following normal public notice and a hearing, on ,

Approved: August 20, 2013

**If requesting discounts for internal connections and basic maintenance for internal connections, the following items need addressed as part of a technology plan. This plan should be approved by the board and filed in the district office. There would be no need to publish it in handbooks.**

*{THE CHILDREN'S INTERNET PROTECTION ACT TECHNOLOGY PLAN}*

*The district's technology plan must be designed with input from district staff who have an understanding of the district's technology level and available resources. The elements of such plan shall include the following:*

- 1) Clear Statement of Goals and a Realistic Strategy for Using Telecommunications and Information Technology to Improve Educational or Library Services;*
- 2) Professional Development Strategy to Ensure Staff Understands How to Use These New Technologies to Improve Education or Library Services;*
- 3) Assessment of the Telecommunication Services, Hardware, Software, and other Services that will be Needed to Improve Education or Library Services; and*
- 4) Evaluation Process that Enables the School or Library to Monitor Progress Toward the Specified Goals and Make Mid-Course Corrections in Response to New Developments and Opportunities as They Arise.*

*\*\*\*This Children's Internet Protection Act Technology Plan must be adopted by the Board of USD \_\_\_395 at a public meeting, following normal public notice and a hearing. Documentation of such adoption including the date thereof (Month Day, Year) must be included in the plan language. \*On District Website ([www.usd395.org](http://www.usd395.org)) under INFORMATION.*

**\*\*\*USD 395 is currently using SONICWALL COMPREHENSIVE GATEWAY SECURITY SUITE for NSA3500 as a filtering agent.**