Peru Public School District #124
CIPA-Compliant Internet Safety Policy

Introduction

It is the policy of Peru Public School District #124 to comply with the Children's Internet Protection Act (Pub. L. No. 106-554) and: **(a)** prevent access by minors to inappropriate material on the Internet and World Wide Web; **(b)** ensure the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications; **(c)** prevent unauthorized access including "hacking" and other unlawful activities by minors online; **(d)** prevent unauthorized disclosure, use, and dissemination of personal information regarding minors; and **(e)** provide filtering measures to restrict minors' access to materials harmful to minors.

Access to Inappropriate Material

(a)(b)(e) 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.

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

The School, either by itself or in combination with the Data Acquisition Site providing Internet access, will utilize filtering software or other technologies to prevent students from accessing visual depictions that are (1) obscene, (2) child pornography, or (3) harmful to minors. It is impossible to control all material and a user may discover inappropriate material. The appropriate response to finding such material is to immediately exit the site, notify the supervising personnel, and not return to that material. The School may also monitor the online activities of students, through direct observation and/or technological means, to ensure that students are not accessing such depictions or any other materials, which is inappropriate for minors.

Inappropriate Network Usage

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

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

In using the computer network and Internet, steps will be taken to ensure that students will not reveal personal information such as home address, telephone number or reveal real last name or any other information, which might allow a person to locate them.

Personally identifiable information concerning students may not be disclosed or used in any way on the Internet without the permission of a parent or guardian. Users should never give out private or confidential information about themselves or others on the Internet, particularly credit card numbers and Social Security numbers. A supervising teacher or administrator may authorize the release of directory information for internal administrative purposes or approved educational projects and activities.

Steps shall be taken to promote the safety and security of users due to vandalism. Vandalism is defined as any malicious attempt to harm or destroy the networks, software, hardware, and data of the District, another user, the Internet, or any other network. This prohibits degrading or disrupting of equipment, software, or system performance. It also includes, but is not limited to, the uploading or creation of malicious software, including computer viruses.

Supervision and Monitoring

(a)(b)(c)(d) It shall be the responsibility of all members of the Peru Public School 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 modification of technology protection measures shall be the responsibility of the Peru Public School District Technology Coordinator or designated representative.

All users and their parents/guardians are advised that access to the electronic network may include the potential for access to materials inappropriate for school-aged pupils. Every user must take responsibility for his or her use of the computer network and Internet and stay away from these sites. If a student finds that other users are visiting offensive or harmful sites, he or she should report such use to the appropriate school personnel.

CIPA Definition of Terms

TECHNOLOGY PROTECTION MEASURE
The tem "technology protection measure" means a specific technology that blocks or filters Internet access to visual depictions that are:
1. OBSCENE, as that term is defined in section 1460 of title18, United States Code;
2. CHILD PORNOGRAPHY, as that term is defined in section 2256 of title 18, United States Code; or
3. Harmful to minors.

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 literacy, artistic, political, or scientific value as to minors.

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