Policy Code: 3226/4205 Internet Safety

A. Introduction

[1] It is the policy of the board to: (a) prevent user access via its technological resources to, or transmission of, inappropriate material on the Internet or through electronic mail or other forms of direct electronic communications; (b) prevent unauthorized access to the Internet and devices or programs connected to or accessible through the Internet; (c) prevent other unlawful online activity; (d) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (e) comply with the Children's Internet Protection Act.

B. Definitions[2]

1. Technology Protection Measure

The term "technology protection measure" means a specific technology that blocks or filters Internet access to visual depictions that are obscene, child pornography, or harmful to minors.

2. Harmful to Minors

The term "harmful to minors" means any picture, image, graphic image file, or other visual depiction that:

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

b. 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

c. taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

3. Child Pornography

The term "child pornography" means any visual depiction, including any photograph, film, video picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where:

a. the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;

b. such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or

c. such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

4. 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.

5. Minor

For purposes of this policy, the term "minor" means any individual who has not attained the age of 17 years.[3]

C. Access to Inappropriate Material[4]

To the extent practical, technology protection measures (or "Internet filters") will be used to block or

filter access to inappropriate information on the Internet and World Wide Web.[5] Specifically, blocking will be applied to audio[6] and visual depictions deemed obscene or to be child pornography or harmful to minors.[7] Student access to other materials that are inappropriate to minors will also be restricted. The board has determined that audio or visual materials that depict violence, nudity, or graphic language that does not serve a legitimate pedagogical purpose are inappropriate for minors.[8] The superintendent, in conjunction with a school technology and media advisory committee (see policy 3200, Selection of Instructional Materials), shall make a determination regarding what other matter or materials are inappropriate for minors.[9] School system personnel may not restrict Internet access to ideas, perspectives, or viewpoints if the restriction is motivated solely by disapproval of the viewpoints involved.

A student or employee must immediately notify the appropriate school official if the student or employee believes that a website or web content that is available to students through the school system's Internet access is obscene, constitutes child pornography, is "harmful to minors" as defined by CIPA, or is otherwise inappropriate for students. Students must notify a teacher or the school principal; employees must notify the superintendent or designee.

Due to the dynamic nature of the Internet, sometimes Internet websites and web material that should not be restricted are blocked by the Internet filter. A student or employee who believes that a website or web content has been improperly blocked by the school system's filter should bring the website to the attention of the principal. The principal shall confer with the technology director to determine whether the site or content should be unblocked. The principal shall notify the student or teacher promptly of the decision. The decision may be appealed through the school system's grievance procedure. (See policies 1740/4010, Student and Parent Grievance Procedure, and 1750/7220, Grievance Procedure for Employees.)

Subject to staff supervision, technology protection measures may be disabled during use by an adult for bona fide research or other lawful purposes.[10]

D. Inappropriate Network Usage

All users of school system technological resources are expected to comply with the requirements established in policy 3225/4312/7320, Technology Responsible Use. In particular, users are prohibited from: (a) attempting to gain unauthorized access, including "hacking" and engaging in other similar unlawful activities; and (b) engaging in the unauthorized disclosure, use, or dissemination of personal identifying information regarding minors.[11]

E. Education, Supervision, and Monitoring

To the extent practical, steps will be taken to promote the safety and security of users of the school system's online computer network, especially when they are using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications. It is the responsibility of all school personnel to educate, supervise, and monitor[12] 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 are the responsibility of the technology director[13] or designated representatives.

The technology director[14] or designated representatives shall provide age-appropriate training for students who use the school system's Internet services. The training provided will be designed to promote the school system's commitment to educating students in digital literacy and citizenship, including:

1. the standards and acceptable use of Internet services as set forth in policy 3225/4312/7320, Technology Responsible Use;

2. student safety with regard to safety on the Internet, appropriate behavior while online, including behavior on social networking websites and in chat rooms, and cyberbullying awareness and response; and[15]

3. compliance with the E-rate requirements of the Children's Internet Protection Act.

Following receipt of this training, the student must acknowledge that he or she received the training, understood it, and will follow the provisions of policy 3225/4312/7320, Technology Responsible Use.[16]

The superintendent shall develop any regulations needed to implement this policy and shall submit any certifications necessary to demonstrate compliance with this policy.

Legal References: Children's Internet Protection Act, 47 U.S.C. 254(h); Neighborhood Children's Internet Protection Act, 47 U.S.C. 254(l); Protecting Children in the 21st Century Act, 47 U.S.C. 254(h)

Cross References: Professional and Staff Development (policy 1610/7800), Student and Parent Grievance Procedure (policy 1740/4010), Grievance Procedure for Employees (policy 1750/7220), Technology in the Educational Program (policy 3220), Technology Responsible Use (policy 3225/4312/7320), School Improvement Plan (policy 3430), Use of Equipment, Materials, and Supplies (policy 6520), Network Security (policy 6524)

Adopted: _____at a public meeting, following normal public notice[17]

Replaces:[18]

Issued: August 29, 2012

Revised: March 28, 2014

Download This Policy Download This Policy With Footnotes

North Carolina School Boards Association

Footnotes

1. This policy is intended to meet the requirements of federal law for receiving universal service discount rates (E-rate) and/or technology funds under the Elementary and Secondary Education Act (ESEA). *See* Children's Internet Protection Act (CIPA), 47 U.S.C. 254 and Elementary and Secondary Education Act, 20 U.S.C. 7131. *The board should ensure that it has a policy that meets these requirements at all times. See* FN 18. E-rate applicants must retain Internet safety policy documentation, including both the policy itself and the adoption records, for a period of ten years after the end of the last funding year that relied on that policy. See 42 C.F.R. 54.516. We recommend that the board consult legal counsel before making changes to this policy to ensure continued compliance with federal requirements.

2. These definitions are found in the Children's Internet Protection Act, 47 U.S.C. 254. In lieu of the detailed definitions included in this section, the board could simply state "*Key terms are as defined in*

the Children's Internet Protection Act."

3. This definition of "minor" is in the Children's Internet Protection Act, 47 U.S.C. 254 (h)(7)(D).

4. The board could add additional precautionary measures such as educating parents, students, and school personnel about the dangers of obscenity and indecency on the Internet or denying use of the Internet until a student reaches an appropriate age. In addition, the board could create more specific guidelines to regulate Internet use.

5. A technology protection measure is required by federal law. 47 U.S.C. 254(h)(5)(B), (C).

6. Blocking of audio materials is not specifically required by law.

7. Social media websites such as Facebook and MySpace are not categorically considered harmful to minors by the FCC and need not be blocked.

8. 47 U.S.C. §254(l)(2). The law requires that "(A) determination of what matter is inappropriate for minors shall be made by the school board (or) local education agency…" The materials listed here are the same ones listed in policy 3225/4312/7320, Technology Responsible Use. The board could specify other types of materials that are deemed inappropriate for minors, or could omit the list altogether and delegate the responsibility for making the determination to the superintendent or other individual(s). We recommend, however, that the board consult legal counsel to review any proposed changes to the language in this section to avoid infringement of students' First Amendment rights.

9. The board could specify a different process for making this determination, or could exclusively establish in policy the types of materials that would be considered inappropriate for minors.

10. 47 U.S.C. 254(h)(5).

11. 47 U.S.C. 254(l).

12. Monitoring the online activities of minors is required by law. 47 U.S.C. 254(h)(5)(B).

13. The appropriate position should be referenced here.

14. The appropriate position should be referenced here.

15. Educating minors on the topics listed here is required by the Protecting Children in the 21st Century Act, 47 U.S.C. 254(h)(5)(B)(iii).

16. A record of training is strongly recommended to demonstrate compliance with legal requirements.

17. Federal law requires that the board's Internet safety policy be adopted following reasonable public notice and at least one public hearing. *See* 47 U.S.C. 254(h)(5)(A), (l)(1).

18. If this policy replaces a prior Internet safety policy (such as NCSBA's model policy 3225/4312/7320, Technology Responsible Use), the title of the original policy and its adoption date should be noted here so that the original adoption date is maintained. E-rate applicants must retain Internet safety policy documentation, including both the policy itself and the adoption records, for a period of ten years after the end of the last funding year that relied on that policy. See 47 C.F.R. 54.516.