Policy Code: 3226/4205 Internet Safety

A. Introduction

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

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.

C. Access to Inappropriate Material

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. Specifically, blocking will be applied to audio and visual depictions deemed obscene or to be child pornography, or harmful to minors. Student access to other materials that are inappropriate for minors will also be restricted. The board has determined that visual materials that depict violence, nudity, or graphic language that does not serve a legitimate pedagogical purpose are inappropriate for minors. The Superintendent, in conjunction with recommendations from school or district staff, shall make a determination regarding what other matters and materials are inappropriate for minors. School system personnel may not restrict Internet access to ideas, perspectives, or viewpoints if the restriction is motivated solely by the 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 administrative staff member, who will then notify the school principal; other school-based employees will notify the principal directly; principals and centrally-based employees must notify the Technology Department.

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 or central office employee shall confer with the technology department 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.

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 unauthorized disclosure.

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 the 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 disabling or otherwise modifying any technology protection measures are the responsibility of the Executive Director of Technology or designated representatives.

The Superintendent 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

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

Following receipt of this training, the student or their teacher must acknowledge that students have received training and will follow the provisions of policy 3225/4312/7320, Technology Responsible Use.

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), Use of Equipment, Materials, and Supplies (policy 6520), Network Security (policy 6524)

Adopted: April 20, 2023

Chapel Hill-Carrboro Schools