Carolina International Charter School

INTERNET SAFETY

AND

CHILDREN'S INTERNET PROTECTION ACT (CIPA) POLICIES AND PROCEDURES

A. INTRODUCTION

Regarding school technology systems, it is the board's policy to: (a) prevent system users access 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 disclosures, including use or dissemination of personal identification information of minors; and (e) comply with the Children's Internet Protection Act (CIPA).

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 or content that meets this three-pronged test

a. taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex or excretion; and
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, the school will use technology protection measures to block or filter access ("blocking") to inappropriate information on the Internet. Specifically, blocking will be applied to audio and visual depictions deemed obscene, child pornography, or harmful to minors. 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. The Head of School shall make a determination regarding what other matter or materials are educationally inappropriate for or harmful to minors. School personnel may not restrict Internet access to ideas, perspectives, or viewpoints if the restriction is motivated, for example, solely by one's social, political moral or religious values, rather than a professional determination of what is educationally appropriate or otherwise harmful (as defined above) to students.

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 Head of School or designee.

Due to the dynamic nature of the Internet, sometimes Internet websites and web material that should not be restricted are inadvertently blocked by an 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 Head of School. The Head of School shall confer with the technology director to determine whether the site or content should be unblocked. The Head of School shall notify the student or teacher promptly of the decision. The decision may be appealed through the school system's grievance procedure. 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 technological resources are expected to comply with the requirements established in the policies governing responsible use. In particular, users are prohibited from: (a) attempting to gain unauthorized access, including "hacking" and engaging in other similar unlawful activities; (b) engaging in the unauthorized disclosure, use, or dissemination of personal identifying information regarding minors; (c) or using the system in any other way that is illegal, harmful to minors, or violates school policies.

E. EDUCATION, SUPERVISION AND MONITORING

To the extent practical, steps will be taken to promote the safety and security of users of the school's online computer network. It is the responsibility of all school instructional personnel to reasonably educate, supervise, and monitor usage of the online computer network and access to the Internet in accordance with this policy.

Procedures for the disabling or otherwise modifying any technology protection measures are the responsibility of the technology director or designated representatives.

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

1. the standards and acceptable use of Internet services as set forth in policies governing 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;
3. compliance with the E-rate requirements of the Children's Internet Protection Act; and
4. the school's right to and practice of monitoring student use of technology systems, and that students have no expectation of privacy in such use.

Following receipt of this training, the student must acknowledge that he or she received the training, understood it, and will follow the provisions of policies governing responsible use.

The Head of School shall develop any regulations or procedures needed to implement this policy and shall submit any certifications necessary to demonstrate compliance with this policy.

Adopted: February 16, 2023