INTERNET SAFETY

A. INTRODUCTION

It is the policy of the Cleveland County Board of Education (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 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 Superintendent, in conjunction with a school Media and Technology Advisory Committee, shall make a determination regarding what other matter or materials are inappropriate for minors.

   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.

D. INAPPROPRIATE NETWORK USAGE
   All users of school system technological resources are expected to comply with the requirements established in policy. 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.

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 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.

Students will be trained in internet safety. School principals shall communicate and enforce an internet safety training program for students. Student training should include instruction about:
1. the standards and acceptable use of Internet services as set forth in Board policy;
2. 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.

School principals or their designee must maintain records that document how the program is implemented at their schools.

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


Adopted: May 14, 2018

Replaces: Board policies 3350, Student Acceptable Use and 5180, Internet Acceptable Use By Employees