

A. INTRODUCTION

It is the policy of the Guilford County Board of Education (the “Board”) to: (a) prevent user access via its technological resources to, or transmission of, inappropriate material on the ~~Internet~~ [internet](#) or through electronic mail or other forms of direct electronic communications; (b) prevent unauthorized access to the ~~Internet~~ [internet](#) and devices or programs connected to or accessible through the ~~Internet~~ [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~~ [internet](#) access to visual depictions that are obscene, constitute 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 [in accordance with applicable law](#); 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~~ [internet](#) filters”) will be used to block or filter access to inappropriate information on the ~~Internet~~ [internet](#) and ~~W~~[world](#) ~~W~~[wide](#) ~~W~~[web](#) and other forms of electronic communications, such as student

email. Specifically, ~~blocking will be applied~~ reasonable precautions will be taken to prevent access to audio and visual depictions deemed obscene or to be child pornography or harmful to minors as well as to websites or web applications that do not protect against the disclosure, use, or dissemination of students' personal information. Student access to other materials that are inappropriate or harmful 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. In addition, students are prohibited from accessing social media platforms, except when expressly directed by a teacher solely for educational purposes.

School system personnel may not restrict ~~Internet~~ internet access to ideas, perspectives, or viewpoints if the restriction is motivated solely by disapproval of the viewpoints involved.

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.

E. EDUCATION, SUPERVISION, AND MONITORING

To the extent practical, steps will be taken to ~~promote~~ protect the safety and security of users of the District'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~~ internet to the extent feasible 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 of or otherwise modifying any technology protection measures are the responsibility of the technology director or designated representatives.

It is the responsibility of all school personnel to educate, supervise, and monitor usage of the online computer network and access to the ~~Internet~~ 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..

Violations of this policy or policy 3225/4312/7320 may result in disciplinary action, including loss of access privileges or other actions defined in Board policy or the Student Code of Conduct for students and personnel action for employees.

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\(h\)](#) ; [G.S. 115C-47\(70\)](#); -102.10

Cross References: ~~Professional and Staff Development (policy 1610/7800)~~ [School Safety \(policy 1510/4200/7270\)](#), Student and Parent Grievance (policy 1740/4010), Employee Grievance (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: April 14, 2020 ~~at a public meeting, following normal public notice~~

Replaces: EFE-P (in part) (issued October 30, 2003)

Revised: [\[date\]](#)

DRAFT