# The Catamount School Policy 3226

## INTERNET SAFETY

*Policy Code:* **3226**

### A. PURPOSE AND POLICY STATEMENT

It is the policy of The Catamount School (School) 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

These definitions are found in the Children's Internet Protection Act, 47 U.S.C. 254 (CIPA).

1. "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" 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" 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" means:
    a. contact between the penis and the vulva, or the penis and the anus, that involves penetration, however slight;
    b. contact between the mouth and the penis, the mouth and the vulva, or the mouth

and the anus;

c. the penetration, however slight, of the anal or genital opening of another by a hand or finger or by any object, with an intent to abuse, humiliate, harass, degrade, or arouse or gratify the sexual desire of any person;
d. intentional touching, not through clothes, of a minor person under 16.

Penetration may be proved by indirect or circumstantial evidence. It is not necessary that the penetration of the genital and anal openings be complete, and emission is not required.

5. "Sexual contact" means an intentional touching, either directly or through the clothing, of the genitalia, anus, groin, breast, inner thigh, or buttocks of any person with an intent to abuse, humiliate, harass, degrade, or arouse or gratify the sexual desire of any person.

6. “Minor” means any Catamount School student 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 audio and visual depictions on the Internet and World Wide Web that are deemed obscene, child pornography, or harmful to minors. Audio or visual materials that depict violence, nudity, or graphic language that does not serve a legitimate pedagogical purpose are inappropriate for minors, and access to those materials will also be restricted. The Dean and Principal shall determine what other matter or materials are inappropriate for minors. School 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 Principal if the student or employee believes that a website or web content that is available to students through the School’s Internet access is obscene, constitutes child pornography, is "harmful to minors" as defined by CIPA and this Policy, or is otherwise inappropriate for students.

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’s filter should bring the website to the attention of the principal. The principal shall confer with the Division of Information Technology to determine whether the site or content should be unblocked. The principal shall notify the student or teacher promptly of the decision.

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 policy 3225, Technology Responsible Use, and University Policy 52, Responsible Use of Information Technology Resources. 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'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.

Procedures for the disabling or otherwise modifying any technology protection measures are the responsibility of the Division of Information Technology or designated representatives under the direction of the Principal or the Dean.

The School 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'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, 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, as needed.

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, Technology Responsible Use.

**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:** Student and Parent Grievance Procedure (policy 1740), Technology Responsible Use (policy 3225)

**Issued:** October 15, 2024