

Hermon School Department

**Internet Safety**

**Introduction**

It is the policy of the Hermon School Department to: (a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)].

**Definitions**

Key terms are as defined in the Children's Internet Protection Act.

**Access to Inappropriate Material**

To the extent practical, technology protection measures (or "Internet filters") shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information.

Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors.

Subject to staff supervision, technology protection measures may be disabled or, in the case of minors, minimized only for bona fide research or other lawful purposes.

**Inappropriate Network Usage**

To the extent practical, steps shall be taken to promote the safety and security of users of the Hermon School Department's network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications.

Specifically, as required by the Children's Internet Protection Act, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called 'hacking,' and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

## **Supervision and Monitoring**

It shall be the responsibility of all members of the Hermon School Department staff overseeing students to supervise and monitor usage of the online computer network and access to the Internet in accordance with this policy and the Children's Internet Protection Act.

Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the Information Services Department or designated representatives.

CIPA definitions of terms:

**TECHNOLOGY PROTECTION MEASURE.** The term "technology protection measure" means a specific technology that blocks or filters Internet access to visual depictions that are:

1. OBSCENE, as that term is defined in section 1460 of title 18, United States Code;
2. CHILD PORNOGRAPHY, as that term is defined in section 2256 of title 18, United States Code; or
3. Harmful to minors.

**HARMFUL TO MINORS.** The term "harmful to minors" means any picture, image, graphic image file, or other visual depiction that:

1. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
2. 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
3. Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

**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.