INTERNET SAFETY POLICY

A policy on internet safety has been a required policy under federal law- the Children's Internet Protection Act (CIPA)- since 2001, as a condition of receiving E-Rate discounts. CIPA was modified under the Broadband Data Services Improvement Act/Protecting Children in the 21st Century Act of 2008 (P.L. 110-385). Under that Act, school districts and BOCES must, as part of their Internet Safety Policy, educate minors about appropriate online behavior, including:

- Interacting with other individuals on social networking sites and in chat rooms; and
- Cyberbullying awareness and response.
    - CIPA requires that school districts that receive E-Rate discounts for Internet access, service or internal connections, and school districts that receive funds under Title III of the Elementary and Secondary Education Act (ESEA), adopt an Internet Safety Policy that provides for and addresses:

1. the use of technology protection measures that block or filter Internet access by minors to visual depictions that are obscene, child pornography, or harmful to minors, and by adults to visual depictions that are obscene or child pornography. An authorized staff member may disabled any such measure during use by an adult conducting bona fide research or other lawful purpose;

2. access by minors to inappropriate matter on the Internet and World Wide Web;

3. the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;

4. the unauthorized access, including "hacking" and other unlawful activities, by minors online;

5. the unauthorized disclosure, use, and dissemination of personal information regarding minors;

6. measures designed to restrict minors' access to materials harmful to minors; and

7. monitoring of the online activities of minors.

The policy must apply to all computers with Internet access, even if they are not accessible by the public. Prior to adoption, the school board must provide reasonable public notice and hold at least one public hearing or meeting to address the proposed policy.

The Board of Education is committed to undertaking efforts that serve to make safe for children the use of district computers for access to the Internet and World Wide Web. To this end, although unable to guarantee that any selected filtering and blocking technology will work perfectly, the Board directs the Superintendent of Schools to procure and implement the use of technology protection measures that block or filter Internet access by:

- adults to visual depictions that are obscene or child pornography, and
- minors to visual depictions that are obscene, child pornography, or harmful to minors, as defined in the Children's Internet Protection Act.

Subject to staff supervision, however, any such measures may be disabled or relaxed for adults conducting bona fide research or other lawful purposes, in accordance with criteria established by the Superintendent or his or her designee.

As indicated above, when adults are using school computers, a teacher or administrator may disable the filtering software to enable access for bona fide research or other lawful

purposes. However, the law does not require that a school district afford adults unfiltered access to the Internet, even for a bona fide request. It is for the Board to determine whether wishes to permit such an exception.

The Superintendent or his or her designee also shall develop and implement procedures that provide for the safety and security of students using electronic mail, chat rooms, and other forms of direct electronic communications; monitoring the online activities of students using district computers; and restricting student access to materials that are harmful to minors.

In addition, the Board prohibits the unauthorized disclosure, use and dissemination of personal information regarding students; unauthorized online access by students, including hacking and other unlawful activities; and access by students to inappropriate matter on the Internet and World Wide Web. The Superintendent or his or her designee shall establish and implement procedures that enforce these restrictions.

The IT network manager designated under the district's Computer Network or Acceptable Use Policy, shall monitor and examine all district computer network activities to ensure compliance with this policy and accompanying regulation. He or she also shall be responsible for ensuring that staff and students receive training on their requirements.

All users of the district's computer network, including access to the Internet and World Wide Web, must understand that use is a privilege, not a right, and that any such use entails responsibility. They must comply with the requirements of this policy and accompanying regulation, in addition to generally accepted rules of network etiquette, and the district's Acceptable Use Policy. Failure to comply may result in disciplinary action including, but not limited to, the revocation of computer access privileges.

As part of this policy, and the district's policy on acceptable use of district computers (policy 4526), the district shall also provide age-appropriate instruction regarding appropriate online behavior, including:

1. interacting with other individuals on social networking sites and in chat rooms, and

2. cyberbullying awareness and response

Instruction will be provided even if the district prohibits students from accessing social networking sites or chat rooms on district computers.

Cross-ref: 4526, Computer Network for Education

Ref: Chidlren's Internet Protection Act, Public Law No. 106-554 47 USC §254 20 USC §6801

Adoption: March 12, 2002
Revised: November 8, 2017
Reviewed: October 11, 2022