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 computer network coordinator 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 date: March 12, 2002
Reviewed: August 8, 2017

Approved: November 8, 2017

INTERNET USE AGREEMENT

Edinburg Common School is committed to optimizing student learning and teaching by providing access to the Internet for all students. Our goal in providing this service is to promote communication, research, and creativity. Internet access is available to students Pre-K-6 grade at **Edinburg Common School and Northville Central School.** We are both very pleased to offer this tool as a valuable resource to both students and teachers for the purpose of conducting research. Students will now have ready access to thousands of libraries. All students will receive Internet instruction which focuses on safety issues as well as how to navigate the Internet to search for information for school-based projects. While we acknowledge that we cannot control the vast amount of information, which is available on the Internet, every effort has been taken toward providing online safety. We invite students and parents to read the "Conditions of Internet Use" section below. Both student and parent signatures are required to access the Internet.

Internet Terms and Conditions

1. Students are responsible for their own behavior on school computers. General school rules for behavior, referenced in the Edinburg Common School **Student Conduct Policy,** will be followed.
2. The Internet is provided for students to conduct research. Access to the Internet is granted to students who agree to conduct themselves in a responsible manner. Access is a privilege. Inappropriate use or behavior on the part of an individual may result in **cancellation** of Internet **privileges** for the **remainder of the year.** Students must always get permission from a teacher or staff member before using the internet.
3. It is forbidden for students to check personal e-mail, face book, and/or instant messaging.
4. Students will be provided one "Flash Drive" at the beginning of the school year, if needed. There will be a five dollar ($5.00) charge for a replacement (if lost or stolen).

Inappropriate use or behavior consists of intentionally damaging computers, attempting to download from the Internet without teacher permission, consistently not attending to teacher instructions, attempting to access inappropriate sites.
Edinburg Common School reserves the right to examine all data stored in computer hard drives to make sure that all users are in compliance with these regulations.

Internet** Use **Agreement

Student Section:

I have read the **Edinburg Common School Internet Use Agreement. I** agree to follow the rules contained in this document. I understand that if I violate any of these rules, I may lose my Internet privileges for the remainder of the school year and I may face other disciplinary measures.

Student's Name: (please print) _____ Grade: _____

Student's Signature: _____ Date: _____

Parent/Guardian Section:

As the parent or legal guardian of the student signing above, I have read the Internet Use Agreement and grant permission for my son or daughter to access the Internet. I understand that Internet access is designed for educational purposes. I also understand that Edinburg Common School cannot be held responsible for sites that are deemed inappropriate but that Edinburg Common School staff has taken every precaution within their power to provide for online safety. I understand that my son or daughter will be held responsible for violations.

Parent/Guardian's Name: (please print) _____ Date: _____
Parent/Guardian's Signature: _____

Adoption date: March 12, 2002

Reviewed: June 9, 2014
Approved: November 8, 2017

INTERNET SAFETY POLICY REGULATION

The following rules and regulations implement the Internet Safety Policy adopted by the Board of Education to make safe for children the use of district computers for access to the Internet and World Wide Web.

I. Definitions

In accordance with the Children's Internet Protection Act,

- *Child pornography* refers to 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 the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct. It also includes any such visual depiction that (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.
- *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.

II. Blocking and Filtering Measures

- The Superintendent or his or her designee shall secure information about, and ensure the purchase or provision of, a technology protection measure that blocks access from all district computers to visual depictions on the Internet and World Wide Web that are obscene, child pornography or harmful to minors.
- The district's computer network coordinator shall be responsible for ensuring the installation and proper use of any Internet blocking and filtering technology protection measure obtained by the district.
- The computer network coordinator or his or her designee may disable or relax the district's Internet blocking and filtering technology measure only for adult staff members conducting research related to the discharge of their official responsibilities.
- The computer network coordinator shall monitor the online activities of adult staff members for whom the blocking and filtering technology measure has been disabled or relaxed to ensure there is not access to visual depictions that are obscene or child pornography.

III. Monitoring of Online Activities

- The district's computer network coordinator shall be responsible for monitoring to ensure that the online activities of staff and students are consistent with the district's Internet Safety Policy and this regulation. He or she may inspect, copy, review, and store at any time, and without prior notice, any and all usage of the district's computer network for accessing the

Internet and World Wide Web and direct electronic communications, as well as any and all information transmitted or received during such use. All users of the district's computer network shall have no expectation of privacy regarding any such materials.

- Except as otherwise authorized under the district's Computer Network or Acceptable Use Policy, students may use the district's computer network to access the Internet and World Wide Web only during supervised class time, study periods or at the school library, and exclusively for research related to their course work.
- Staff supervising students using district computers shall help to monitor student online activities to ensure students access the Internet and World Wide Web, and/or participate in authorized forms of direct electronic communications in accordance with the district's Internet Safety Policy and this regulation.
- The district's computer network coordinator shall monitor student online activities to ensure students are not engaging in hacking (gaining or attempting to gain unauthorized access to other computers or computer systems), and other unlawful activities.

IV. Training

- The district's computer network coordinator shall provide training to staff and students on the requirements of the Internet Safety Policy and this regulation at the beginning of each school year.
- The training of staff and students shall highlight the various activities prohibited by the Internet Safety Policy, and the responsibility of staff to monitor student online activities to ensure compliance therewith.
- Students shall be directed to consult with their classroom teacher if they are unsure whether their contemplated activities when accessing the Internet or Worldwide Web are directly related to their course work.
- Staff and students will be advised to not disclose, use and disseminate personal information about students when accessing the Internet or engaging in authorized forms of direct electronic communications.
- Staff and students will also be informed of the range of possible consequences attendant to a violation of the Internet Safety Policy and this regulation.

V. Reporting of Violations

- Violations of the Internet Safety Policy and this regulation by students and staff shall be reported to the Building Principal.
- The Principal shall take appropriate corrective action in accordance with authorized disciplinary procedures.
- Penalties may include, but are not limited to, the revocation of computer access privileges, as well as school suspension in the case of students and disciplinary charges in the case of teachers.

Adoption date: March 12, 2002
Reviewed: June 9, 2014

Approved: November 8, 2017