

## COMPUTER NETWORK FOR EDUCATION

The Board of Trustees is committed to optimizing student learning and teaching. The Board considers student access to a computer network, including the Internet, to be a powerful and valuable educational and research tool, and encourages the use of computers and computer-related technology in district classrooms solely for the purpose of advancing and promoting learning and teaching.

The computer network can provide a forum for learning various software applications and through online databases, bulletin boards and electronic mail, can significantly enhance educational experiences and provide statewide, national and global communication opportunities for staff and students.

All users of the district's computer network and the Internet must understand that use is a privilege, not a right, and that use entails responsibility.

The Superintendent shall establish regulations governing the use and security of the district's computer network. All users of the district's computer network and equipment shall comply with this policy and those regulations. Failure to comply may result in disciplinary action as well as suspension and/or revocation of computer access privileges.

The Superintendent shall be responsible for designating a computer network coordinator to oversee the use of district computer resources. The computer coordinator will prepare in-service programs for the training and development of district staff in computer skills, and for the incorporation of computer use in appropriate subject areas.

The Superintendent, working in conjunction with the designated purchasing agent for the district, the computer network coordinator and the instructional materials planning committee, will be responsible for the purchase and distribution of computer software and hardware throughout district schools. They shall prepare and submit for the Board's approval a comprehensive multi-year technology plan which shall be revised as necessary to reflect changing technology and/or district needs.

Cross-ref: 4319, Science and Math Instruction

Adoption date: December 10, 1998

Reviewed: June 9, 2014

## COMPUTER NETWORK FOR EDUCATION REGULATION

The following rules and regulations govern the use of the district's computer network system and access to the Internet.

### *I. Administration*

- The Superintendent shall designate a computer network coordinator to oversee the district's computer network.
- The computer network coordinator shall monitor and examine all network activities, as appropriate, to ensure proper use of the system.
- The computer network coordinator shall be responsible for disseminating and interpreting district policy and regulations governing use of the district's network at the building level with all network users.
- The computer network coordinator shall provide employee training for proper use of the network and will ensure that staff supervising students using the district's network provide similar training to their students, including providing copies of district policy and regulations governing use of the district's network.
- The computer network coordinator shall ensure that all disks and software loaded onto the computer network have been scanned for computer viruses.
- All student agreements to abide by district policy and regulations and parental consent forms shall be kept on file in the district office.

### *II. Internet Access*

*[Note: The School Board should amend these access provisions as appropriate]*

- 6th grade students will be provided access: during selected computer and class time; during instructional time in a controlled environment.
- 6th grade students may browse the World Wide Web:
- 6th grade students are not to participate in chat rooms.
- Students may construct their own web pages using district computer resources under supervision and instruction.
- 6th grade students will have computer e-mail address.
- 6th grade students are not allowed to belong to mailing lists
- A staff member will be required to monitor all of these activities.

### *III. Acceptable Use and Conduct*

- Access to the district's computer network is provided solely for educational purposes and research consistent with the district's mission and goals.
- Use of the district's computer network is a privilege, not a right. Inappropriate use may result in the suspension or revocation of that privilege.
- Each individual in whose name an access account is issued is responsible at all times for its proper use.

- All network users will be issued a login name and password. Passwords must be changed periodically.
- Only those network users with written permission from the Superintendent or computer network coordinator may access the district's system from off-site (e.g., from home).
- All network users are expected to abide by the generally accepted rules of network etiquette. This includes being polite and using only appropriate language. Abusive language, vulgarities and swear words are all inappropriate.
- Network users identifying a security problem on the district's network must notify the appropriate teacher, administrator or computer network coordinator. Under no circumstance should the user demonstrate the problem to anyone other than to the district official or employee being notified.
- Any network user identified as a security risk or having a history of violations of district computer use guidelines may be denied access to the district's network.

#### IV. *Prohibited Activity and Uses*

The following is a list of prohibited activity concerning use of the district's computer network. Violation of any of these prohibitions may result in discipline or other appropriate penalty, including suspension or revocation of a user's access to the network.

- Using the network for commercial activity, including advertising.
- Infringing on any copyrights or other intellectual property rights, including copying, installing, receiving, transmitting or making available any copyrighted software on the district computer network.
- Using the network to receive, transmit or make available to others obscene, offensive, or sexually explicit material.
- Using the network to receive, transmit or make available to others messages that are racist, sexist, abusive or harassing to others.
- Using another user's account or password.
- Attempting to read, delete, copy or modify the electronic mail (e-mail) of other system users and deliberately interfering with the ability of other system users to send and/or receive e-mail.
- Forging or attempting to forge e-mail messages.
- Engaging in vandalism. Vandalism is defined as any malicious attempt to harm or destroy district equipment or materials, data of another user of the district's network or of any of the entities or other networks that are connected to the Internet. This includes, but is not limited to, creating and/or placing a computer virus on the network.
- Using the network to send anonymous messages or files.

- Using the network to receive, transmit or make available to others a message that is inconsistent with the district's Code of Conduct.
- Revealing the personal address, telephone number or other personal information of oneself or another person.
- Using the network for sending and/or receiving personal messages.
- Intentionally disrupting network traffic or crashing the network and connected systems.
- Installing personal software or using personal disks on the district s computers and/or network without the permission of the appropriate district official or employee.
- Using district computing resources for commercial or financial gain or fraud.
- Stealing data, equipment or intellectual property.
- Gaining or seeking to gain unauthorized access to any files, resources, or computer or phone systems, or vandalize the data of another user.
- Wastefully using finite district resources.
- Changing or exceeding resource quotas as set by the district without the permission of the appropriate district official or employee.
- Using the network while access privileges are suspended or revoked.
- Using the network in a fashion inconsistent with directions from teachers and other staff and generally accepted network etiquette.

#### V. *No Privacy Guarantee*

Students using the district  or computer network should  
 does the district guarantee privacy for electronic mail (e-mail) or any use of the  
 district s computer network  
 any material stored on district equipment or any material used in conjunction with  
 the district s computer network.

#### VI. *Sanctions*

All users of the district's computer network and equipment are required to comply with the district's policy and regulations governing the district's computer network. Failure to comply with the policy or regulation may result in disciplinary action as well as suspension and/or revocation of computer access privileges.

In addition, illegal activities are strictly prohibited. Any information pertaining to or implicating illegal activity will be reported to the proper authorities. Transmission of any material in violation of any federal, state and/or local law or regulation is prohibited. This includes, but is not limited to materials protected by copyright, threatening or obscene material or material protected by trade secret. Users must respect all intellectual and property rights and laws.

*VII. District Responsibilities*

The district makes no warranties of any kind, either expressed or implied, for the access being provided. Further, the district assumes no responsibility for the quality, availability, accuracy, nature or reliability of the service and/or information provided. Users of the district's computer network and the Internet use information at their own risk. Each user is responsible for verifying the integrity and authenticity of the information that is used and provided.

The district will not be responsible for any damages suffered by any user, including, but not limited to, loss of data resulting from delays, non-deliveries, misdeliveries, or service interruptions caused by its own negligence or the errors or omissions of any user. The district also will not be responsible for unauthorized financial obligations resulting from the use of or access to the district's computer network or the Internet.

Further, even though the district may use technical or manual means to regulate access and information, these methods do not provide a foolproof means of enforcing the provisions of the district policy and regulation.

Adoption date: December 10, 1998

Reviewed: June 9, 2014

**COMPUTER NETWORK FOR EDUCATION EXHIBIT**

## Parent/Guardian Letter

Dear Parent/Guardian:

The district would like to offer your child access to our educational computer network, including the Internet. With your permission, your child will have access to various software applications, hundreds of databases, libraries and computer services from all over the world through the Internet and other electronic information systems.

The Internet is a system which links smaller networks creating a large and diverse network. The Internet allows students the opportunity to reach out to many other people to share information, learn concepts, and research subjects by the sending and receiving of messages using a computer, modem and phone lines.

With this educational opportunity also comes responsibility. It is important that you and your child read the enclosed district Computer Network for Education policy, regulation and consent and waiver form and discuss these requirements together. You and your child should understand that inappropriate network use will result in the loss of the privilege to use this educational tool.

As indicated in the enclosed policy and regulation, the district will attempt to discourage access to objectionable material and communications. However, in spite of our efforts to establish regulations governing use of the district's computer network and student access to the Internet, a variety of inappropriate and offensive materials are available over the Internet and it may be possible for your child to access these materials inadvertently or if he/she chooses to behave irresponsibly. In addition, it is possible for undesirable or ill-intended individuals to communicate with your child over the Internet. There is no practical means for the district to prevent this from happening, and your child must take responsibility to avoid such communications if they are initiated.

I have included the above information to ensure that your decision regarding your child's access to the district's computer network and the Internet is an informed one. You must be the one to decide whether the benefits of your child having access to the district's computer network and the Internet outweigh the potential risks.

If you wish to allow your child access to the district's computer network and the Internet, please return the enclosed consent and waiver form to me.

Sincerely,

Superintendent

Adoption date: December 10, 1998

Reviewed: June 9, 2014

## INTERNET SAFETY 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.

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.

Cross-ref: 4526, Computer Network for Education

Ref: Public Law No. 106-554  
47 USC §254  
20 USC §6801

Adoption date: March 12, 2002

Reviewed: June 9, 2014

## 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) is, or appears to be, of a minor engaging in sexually explicit conduct; or (b) has been created, adapted or modified to appear that an identifiable minor is engaging in sexually explicit conduct; or (c) is advertised, promoted, presented, described, or distributed in such a manner that conveys the impression that the material is or contains a visual depiction of a minor 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

## 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