COMPUTER NETWORK AND INTERNET USE POLICY

As modern educational institutions striving for excellence, the Big Foot Area Schools have a responsibility to provide its students and staff with excellent and appropriate access to computer information systems commensurate with their educational needs. The school community must respect information and use computer technologies ethically.

Technology is the property of the Sharon Jt. 11 School District and is provided for students and staff to help achieve excellence in education. Technology includes computer facilities, all hardware and software, the Internet, e-mail, phone and voicemail systems, audio/video equipment, peripherals, networks, servers, telecommunications, and related services. Our goal in providing these services to staff and students is to promote learning, facilitating resource sharing, innovation, and communication.

Through network access, learners will:

- utilize a personalized, motivational learning opportunity
- enter into partnerships to enhance their learning options
- gain an employability skill needed for the 21st century
- broaden their problem-solving and decision-making abilities
- broaden their research capabilities by using primary materials
- develop their higher-level thinking skills
- access global resources.

Access is a privilege, not a right. Realizing that no filtering device is 100% effective, the Sharon Jt. 11 School District will make every effort to purchase and continuously maintain an effective filtering service. The district acknowledges the potential exposure to obscene or objectionable material is not and cannot be entirely avoided. The Sharon Jt. 11 School District requires parent or guardian approval before a student is allowed to use the Internet at school. A signed Acceptable Use Agreement must be on file with the network administrator before a student or staff member will be permitted to access the Internet from a school district computer. For security purposes, all authorized users will be issued user accounts and passwords that are age appropriate, which they will be required to use.

Access entails responsibility. Students and staff are responsible for good behavior on the Board's technology equipment and the Internet just as they are in classrooms, school hallways, and other school premises and school sponsored events. Communications on the Internet are often public in nature. General school rules for behavior and communication apply. The Board does not sanction any use of the Internet that is not authorized by or conducted strictly in compliance with this policy and its accompanying guidelines. Users who disregard this policy and its accompanying guidelines may have their use privileges suspended or revoked, and disciplinary action taken against them. Users granted access to the Internet through the Board's

equipment assumes personal responsibility and liability, both civil and criminal, for uses of the Internet not authorized by this Board policy and its accompanying guidelines.

Utilization of technology for non-school related purposes may occur, but only to a reasonable degree. All users must be aware that personal privacy is not, and cannot be guaranteed.

User accounts may be treated like school lockers (Legal Reference: WI Statute 118.32 and 118.324). Technology administrators may review files and communications to maintain system integrity and ensure that users are using the system responsibly.

Furthermore, the district does not warrant network functionality and is not responsible for any information that may be lost, damaged or irretrievable when using the network. Likewise, the district does not guarantee the accuracy of information received via the Internet by its users.

It is impossible to completely define unacceptable use, however, for the purpose of illustration, some examples are:

- Sending or displaying offensive messages or pictures;
- Using offensive or obscene language;
- Harassing, insulting, threatening or attacking others, including racial or sexual slurs (i.e. cyber bullying);
- Damaging equipment or networks;
- Plagiarism and violating copyright laws;
- Using others' passwords;
- Trespassing in others' folders, work or files;
- Unauthorized access such as hacking;
- Intentionally wasting resources;
- Regularly employing the technology for commercial, political or religious purposes;
- Illegal activities;
- Unauthorized installation of software.

Users are responsible for reporting occurrences of unacceptable use to school staff or officials.

Sanctions

1. Violations may result in usage restriction including loss of access to the Internet, and/or user account/files.
2. Additional disciplinary action (i.e. suspension) may be determined at the building and/or district level in line with existing practice regarding inappropriate behavior.
3. When applicable, law enforcement agencies may be involved.

Internet Safety (CIPA and NCIPA-Compliant)

Introduction

It is the policy of the Sharon Jt. 11 School District, as a member of the Big Foot Area Schools Consortium, to make a good faith effort to: (a) prevent user (students, staff, minors, adults)

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, including so-called hacking, 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)] and the Neighborhood Children's Internet Protection Act (NCIPA).

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. Recognizing that no internet filtering device is 100% effective, the District acknowledges that the potential exposure to inappropriate information is not and cannot be entirely avoided. It is impossible to guarantee students will not gain access through the Internet to information and communications that they and/or their parents/guardians may find inappropriate, offensive, objectionable or controversial. A student, staff member, parent or citizen may complain, either to school administration or directly to the FCC if banned material repeatedly gets through the filter.

Inappropriate Network Usage

To the extent practical, steps shall be taken to promote the safety and security of users of the Sharon Jt. 11 School District online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications (whether use is intended or accidental).

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.

Education, Supervision and Monitoring

It shall be the responsibility of all instructional members of the Sharon Jt. 11 School District staff to educate, supervise and monitor appropriate use 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 (Pub. L. No. 110-385 Title II).

The Sharon Jt. 11 School District will promote safe online activity for children and educate students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyber bullying awareness and response. This includes, but is not limited to:

- Teaching students how to locate and evaluate appropriate electronic sources.
- Teaching students information literacy skills, including understanding of safety, copyright, ethical practice and data privacy.
- Teaching students proper safety procedures when using electronic mail, chat rooms, social networking websites, cyber bullying awareness and response, and other forms of direct electronic communication.

For the safety of our students, the school district's Internet content filter is programmed to block student access to, among others, popular social networking sites (MySpace, Facebook, etc.). Students are also prohibited from using private email services (Hotmail, Google Mail, etc.) and instant messaging software or services (Microsoft Instant Messenger, ichat, Skype, etc.) while using the district's network unless directly relate to classroom activities and only under the direct supervision of a teacher.

Students' home and personal Internet use can have an impact on the school district and on other students. If student's personal Internet expression, such as a threatening message to a staff member or another student, or a website advocating violence or defamation of another's character, creates a substantial disruption, offenders will be subject to disciplinary and legal actions. Substantial disruption is defined as any of the following: (a) necessary cessation of instruction or educational activities; (b) inability of students or educational staff to focus on learning or function as an educational unit because of a hostile environment; (c) severe or repetitive disciplinary measures are needed in the classroom or during educational activities; or (d) exhibition of other behavior by students of educational staff that substantially interfere with the learning environment. (AR Legislature, Public Act 115).

Procedures for disabling or otherwise modifying any technology protection measures shall be the responsibility of the Technology Coordinator and Network Systems Specialist under the direction of the District Administrator.

Definitions

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

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.

Legal Reference:	Sections	19.84	Wisconsin Statutes
		120.13(1)	Wisconsin Statutes
		943.70	Wisconsin Statutes
		947.125	Wisconsin Statutes
		118.32	Wisconsin Statutes
		118.324	Wisconsin Statutes
	Section	106-554; 47 USC 254 (h)(5)(b); S. 1492[110th]	
Cross-Reference:	Exhibit 362.3 – Children's Internet Protection Act – Public Law 106-554 and 47 USC 254(h)(5)(b), Protecting Children in the 21st Century Act – Pub. L. No. 110-385 Title II, and Broadband Data Improvement Act 2008 – S. 1492[110th]; Policy 363 – Copyright Regulations; Exhibit 363 – Copyright Guidelines; Policy 361 – Instructional Resources		

Policy Adopted: October 31, 2005
Policy Approved: January 10, 2006
Policy Revised: September 13, 2010
Policy Revised: August 14, 2012