Washington West Supervisory Union Model Policy

Policy G11-R[1]

G11-R: ACCEPTABLE USE OF ELECTRONIC RESOURCES & THE INTERNET

Purpose

It is the policy of the member district schools of the Washington West Supervisory Union: Fayston Elementary School, Harwood Union High School, Moretown Elementary School, Waitsfield Elementary School, Warren Elementary School, and the Waterbury/Duxbury Union School District (Crossett Brook Middle School and Thatcher Brook Primary School) to set standards for the responsible use of electronic resources.

Computers, electronic devices and the Internet provide access to vast, diverse, and unique resources in a global community. Our goal in providing students, teachers, and staff access to electronic tools, a computer network, and the Internet is to promote educational excellence in each of the member district schools of the Washington West Supervisory Union: Fayston Elementary School, Harwood Union High School, Moretown Elementary School, Waitsfield Elementary School, Warren Elementary School, and the Waterbury/Duxbury Union School District (Crossett Brook Middle School and Thatcher Brook Primary School).

This policy is intended to ensure compliance with the requirements of applicable federal and state laws that regulate the provision of access to the internet and other electronic resources by school districts. This policy complies with the statutory requirements of the Children's Internet Protection Act (CIPA) and promotes the safe, ethical, responsible, and legal use of electronic resources including the Internet to support the effective use of these resources for educational purposes. CIPA requires the installation and use of filtering software or services on all computers with access to the Internet to prevent access to visual depictions of obscenity, child pornography or other materials harmful to minors.

Definitions

As used in this policy, the following terms shall be defined in accord with federal and, where the context clearly allows, state law.

1) **Child Pornography** means 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:
    - **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 create, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.[2]

2) **Harmful to minors** means any picture, image, graphic image file or other visual depiction that:
    - **a.** Taken as a whole, 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 lewd exhibition of the genitals; and
    - **c.** Taken as a whole lacks serious literary, artistic, political or scientific value as to minors.[3]
3) **Technology protection measure** means a specific technology that blocks or filters Internet access to visual depictions that are obscene, child pornography or harmful to minors.[4]
4) **Minor** means an individual who has not attained the age of 18.[5]
5) **Computer** means any hardware, software, or other technology attached or connected to, installed in, or otherwise used in connection with a computer.[6]
6) **Access to Internet** means a computer that is equipped with a modem or is connected to a computer network that has access to the Internet.[7]

Policy

Access to member district electronic resources within or outside the school setting, including the Internet, will be available to students and staff who agree to abide by the requirements of this policy and to act in a considerate and responsible manner. User agreements, except as otherwise described in this policy, will be required prior to allowing any individual unsupervised access to member district electronic resources. All electronic devices and computers are to be used in a responsible, efficient, ethical, and legal manner. Personal electronic devices used at a district school are subject to the same expectations.

Violation of this policy and the procedures developed in accordance with this policy may result in disciplinary action or referral to local, state or federal law enforcement officials.

The availability of access to electronic information does not imply endorsement by the member district of the content, nor does the member district guarantee the accuracy of information received. The member district shall not be responsible for any information that may be lost, damaged or unavailable when using the network or for the content of any information that is retrieved via the internet.

The use by students, staff or others of district electronic resources is a privilege, not a right. The member district's computer and network resources are the property of the member district. Users shall have no expectation of privacy in anything they create, store, send, receive or display on or over the member district's computers or network resources, including personal files. The member district reserves the right to monitor, track, and log network access and use; monitor fileserver space utilization by member district users; or deny access to prevent unauthorized, inappropriate or illegal activity and may revoke access privileges and/or administer appropriate disciplinary action for misuse of its electronic resources. The member district shall cooperate to the extent legally required with local, state and federal officials in any investigation concerning or related to the misuse of the member district's Internet, computers or network.

The district shall work to ensure Internet safety for minors by taking steps that include monitoring the online activities of minors and the operation of technology protection measures with respect to any of its computers with Internet access that protects against access through such computers to visual depictions that are obscene, child pornography or harmful to minors.[8]

The following materials, in addition to those stated in law and defined in this policy, are inappropriate for access by minors:

- Defamatory
- Lewd, vulgar, or profane
- Threatening
- Harassing or discriminatory
- Bullying
- Terroristic

The district shall operate technology protection measures during the use of any of its computers with Internet access, including those computers not accessible to minors, that protect against access through such computers to material inappropriate for minors, including but not limited to, visual depictions that are obscene or child pornography.[9]

Administrative Responsibilities

The Superintendent or designee will coordinate and oversee the use of member district electronic resources including the Internet. The Principal or designee will serve as the building-level coordinator for use of the electronic resources including the Internet and will develop building-level procedures necessary to implement this policy. The procedures will include provision for educators to receive proper training, guidelines for the supervision of students using the system, monitoring the use of the system, and overseeing management of the "Responsible use procedures" agreement process. In addition, the Principal or his or her designee shall ensure that the member district, as part of its implementation of this policy, is educating minors about appropriate on-line behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.[10]

The member districts will stipulate in any agreement or contract that Internet service providers will not collect, analyze, and/or sell individual or anonymous student use data for the purpose of commercial advertising and marketing research activities. The collection and analysis of student use data strictly for the purpose of evaluating the educational success of the electronic resources is allowed, provided that student confidentiality standards are maintained.

In addition, the administrative procedures developed under this policy shall include Internet safety measures that provide for the monitoring of online activities by minors[11] and address the following:

1. Control of access by minors to inappropriate matter on the Internet and World Wide Web.
2. Safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications.
3. Prevention of unauthorized online access by minors, including "hacking" and other unlawful activities.
4. Unauthorized disclosure, use, dissemination of personal information regarding minors.
5. Restriction of minors' access to materials harmful to them.[12]

The administrative procedures developed under this policy shall also provide that authorized individuals may temporarily disable the member district's technology protection measures to enable access for bona fide research or other lawful purpose.[13]

The Superintendent or his or her designee shall conduct a regular analysis of the implementation of this policy, and shall make recommendations to the Board as needed to ensure that the member district's approach to Internet safety is effective.

Staff Responsibilities

School staff members are responsible for assuring that students are instructed and supervised in a manner that is both appropriate to the age of the students, and considers the circumstances regarding the use of electronic resources including the Internet. The Principal or designee will develop and disseminate staff supervision guidelines for their respective schools.

Student electronic records are confidential and should be treated like all other student records.

User Responsibilities

During school hours, student users may access electronic resources including the Internet for educational purposes only. The term "educational purpose" includes use of the system for classroom activities, which may involve e-mail communication, career development, and curriculum driven research. It also includes use of the system for other school activities such as sports, other co-curricular activities and school sponsored fund raising activities.

Students agree to follow communication safety protocol outlined in administrative procedures when using electronic communications including the Internet.

Students and staff may access the District's electronic resources for limited personal use. Limited personal use of the District's electronic resources including the Internet shall be allowed if permission is granted by the superintendent or his or her designee in advance, and the use:

- imposes no tangible cost to the District;
- does not unduly burden the District's electronic resources;
- occurs during non-instructional time and does not impede other student or staff access for educational purposes; and
- does not violate this policy

Users will respect the rights of copyright owners and will not plagiarize works they find on the member district's electronic network including the Internet by presenting them as their own.

Users will not intentionally interfere with individual computer or network system performance or attempt to access another person's account, files, or password. Individuals may be denied access to the system based upon security violations of any computer system.

Users should not expect that any files and records of their online activity created on the member district's system are private. Users will be informed about the member district's supervision and monitoring activities and the limitations on their privacy.

Students and staff may not access materials for any purpose that the member district deems to be potentially harmful, inappropriate, or illegal. This includes materials that are obscene or child pornography.

All users of District electronic resources are expected to act in a responsible, ethical and legal manner. Specifically, the following uses are prohibited:

1. Commercial or for-profit uses.
2. Product advertisement or political lobbying.
3. Bullying or harassment[14]
4. Offensive or inflammatory communication, including hate mail, discriminatory remarks or "sexting."[15]

5. Unauthorized or illegal installation, distribution, reproduction or use of copyrighted materials.
6. Accessing sending, receiving, transferring, viewing sharing or downloading obscene, pornographic, lewd or otherwise illegal materials, images or photographs.
7. Inappropriate language or profanity.[16]
8. Impersonation of another user.
9. Loading or using unauthorized games, programs, files or other electronic media.
10. Disabling or bypassing the Internet blocking/filtering software without authorization.
11. Accessing, sending, receiving, transferring, viewing, sharing or downloading confidential information without authorization.

Parental Notification and Responsibility

Each member district school will provide written notice to parents/guardians about student use of member district electronic resources including the Internet, the policies and procedures governing their use, and the limitation of liability of the member district.

Limitation/Disclaimer of Liability

The member districts are not liable for unacceptable use or violations of copyright restrictions or other laws, user mistakes or negligence, and costs incurred by users. The member districts are not responsible for ensuring the accuracy, age appropriateness, or usability of any information found on the member district's electronic resources network including the Internet.

The member districts are not responsible for any damage experienced, including, but not limited to, loss of data or interruptions of service. The member districts are not responsible for the accuracy or quality of information obtained through or stored on the electronic resources system including the Internet, or for financial obligations arising through their unauthorized use.

Date Warned:	09.06.12
Date Adopted:	FES: 09.18.12; HUHS: 09.19.12; MES: 09.10.12; W-D: 09.11.12; WES: 09.17.12; WS: 09.19.12
Legal Reference(s):	15 U.S.C. §6501 (Children's Online Privacy Protection Act)
	17 U.S.C. §§101-120 (Federal Copyright Act of 1976 as amended)
	20 U.S.C. § 6777 et seq. (Enhancing Education Through Technology Act)
	18 U.S.C. §2251 (Federal Child Pornography Law—Sexual Exploitation and Other Abuse of Children)
	47 U.S.C. §230 (Computer Decency Act)
	47 U.S.C. §254 (Children's Internet Protection Act)
	47 CFR §54.520 (CIPA Certifications)
	13 V.S.A. §§2802 et seq. (Obscenity, minors)
	13 V.S.A. § 1027 (Disturbing Peace by Use of…Electronic Means)
	13 V.S.A. §2605 (Voyeurism)
Cross Reference:	Student Conduct and Discipline (F1)
	Copyrights (G2)
	Selection of Instructional Materials (G5)
	Complaints About Instructional Materials (G6)

[1] The federal No Child Left Behind Act (NCLBA) makes schools ineligible to receive funding for the purchase of computers used to access the internet, or to pay costs associated with accessing the internet, through the technology grants program "…unless the school, school board, local educational agency, or other authority with responsibility for administration of (the) school both…has in place a policy of Internet safety for minors that includes the operation of a technology protection measure with respect to any of its computers with Internet access that protects against access through such computers to visual depictions that are…obscene; child pornography; or harmful to minors; and is enforcing the operation of such computers by minors; and has in place a policy of Internet safety that includes the operation of a technology protection measure with respect to any of its computers with Internet access that protects against access through such computers to visual depictions that are…obscene or child pornography and is enforcing…such measure during use of any such computers…" 20 U.S.C. § 6777; 47 U.S.C. § 254(h)(5)(A) & (B). Prior to adoption, the school must "provide reasonable public notice and hold at least one public hearing or meeting to address the proposed Internet safety policy." 47 U.S.C. § 254(l)(1)(B).

[2] 18 U.S.C. § 2256. See, 13 V.S.A. § 2801(6) for the state definition of this term. Federal law requires the use of the federal definition in this policy.

[3] Federal law defines "minor" as a person who has not yet attained the age of 17. 20 U.S.C. § 6777; 47 U.S.C. § 254. Vermont's anti-obscenity law defines the term "minor" as "any person less than 18 years old." 13 V.S.A. § 2801(1). The Vermont definition is used in this model policy as it includes the federal requirement and also provides coverage for students until they reach the age of 18.

[4] 47 U.S.C. § 254

[5] See footnote 3 above.

[6] 20 U.S.C. § 6777(e)(1)

[7] 20 U.S.C. § 6777(e)(2)

[8] 47 U.S.C. § 254(h)(B)

[9] 20 U.S.C. § 6777(a)(2)(A); 47 U.S.C. § 254

[10] Required by 47 U.S.C. § 254(h)(5)(B)

[11] Required by 47 U.S,C. § 254(h); 47 C.F.R. § 54.520(C)(i)

[12] Required by 47 U.S.C. § 254(1); 47 C.F.R. § 54.520(c)(ii)

[13] Required by 20 U.S.C. § 6777(c)

[14] 13 V.S.A. § 1027 makes it a crime in Vermont to "disturb peace by use of telephone or other electronic communications." Actionable activities under the statute include threatening, harassing, intimidating communications as well as the use of "obscene, lewd, lascivious or indecent language" with intent to harass or intimidate by telephone or other electronic communication.

[15] 13 V.S.A. § 2802b makes activities commonly referred to as "sexting" by minors illegal in Vermont.

[16] 13 V.S.A. § 2605 makes "voyeurism" illegal in Vermont.