WALWORTH POLICY 363.2

TECHNOLOGY USE AND NETWORK ACCESS POLICY

As modern educational institutions striving for excellence, The Walworth Joint School District #1 has a responsibility to provide excellent and appropriate technology and network access. The policy provides the school community with guidelines associated with the use of District technology and network access. These guidelines apply to any user of the District’s technology or network access including, but not limited to, students, staff, and guests. Users must respect and use computer technologies effectively

Technology Use

Technology is the property of the Walworth Jt. District #1 and is provided for students, staff, and guests to help achieve excellence in education. Technology includes, but not limited to, computer facilities, all hardware and software, the Internet, e-mail, phone and voicemail systems, audio/video equipment, peripherals, networks, servers, telecommunications, and related services. Walworth Joint District #1 recognizes that technology and information systems are ever-changing and evolving. Our goal in providing these technologies is to promote and facilitate learning, facilitate resource sharing, innovation, and communication within the perimeters of available funding. .

Internet Access

Internet Access is a privilege and with that comes personal accountability and responsibility for appropriate use and behavior. Users are responsible for appropriate digital citizenship when using technology equipment and the Internet. Communication on the Internet is often public in nature. General school rules for behavior and communication apply.

A signed Acceptable Use Agreement must be on file with the District before a student or staff member will be permitted to use technology and web-based resources. For security purposes, all authorized users will be issued user accounts and passwords. Guest Users will need to accept the User Agreement before having access to the Internet.

User accounts may be treated like school lockers (Legal Reference: WI Statute 118.32 and 118.324). Technology District administrators or their designee may review files and communications to maintain system integrity and ensure that users are using the system responsibly. All use is subject to provisions of the state public records law. Deletion of a message does not protect privacy. The District may monitor email for school District communication purposes.

Walworth Jt. District #1 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 disciplinary action taken against them.

Users who are granted access to the Internet through the District’s equipment assume personal responsibility and liability, both civil and criminal, for uses of the Internet not authorized by this policy and its accompanying guidelines.

Utilization of technology and/or internet access 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.

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:

1. Sending or displaying offensive messages or pictures;
2. Using offensive or obscene language;
3. Harassing, insulting, threatening or attacking others, including racial or sexual slurs (i.e. cyberbullying);
4. Damaging equipment or networks;
5. Plagiarism and violating copyright laws;
6. Using others’ passwords;
7. Trespassing in others’ folders, work or files;
8. Unauthorized access such as hacking;
9. Intentionally wasting resources;
10. Regularly employing the technology for commercial, political or religious purposes;
11. Illegal activities; and,
12. Unauthorized installation of software.

Users are responsible for reporting occurrences of unacceptable use to the appropriate school staff or officials. Students should report occurrences to their teacher. Staff should report occurrences to the Technology Coordinator. Guests should report occurrences to the District Administrator.

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 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 Walworth Jt. District #1 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, or parent may report their concerns to administration 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 Walworth Jt. District #1 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 Walworth Jt. District #1 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 Walworth Jt. District #1 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 cyberbullying awareness and response. This includes, but is not limited to:

*1.* *Teaching students how to locate and evaluate appropriate electronic sources.*

*2.* *Teaching students information literacy skills, including understanding of safety, copyright, ethical practice and data privacy.*

*3.* *Teaching students proper safety procedures when using electronic mail, chat rooms, social networking websites, cyberbullying 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.

Walworth Jt. District #1 does not discriminate on admissions to any school, class, program, or activity on the basis of sex, race, religion, national origin, creed, pregnancy, marital status, parental status, sexual orientation, or physical, learning, emotional, or mental disability. All discrimination complaints shall be processed in accordance with established procedures.

**LEGAL REFERENCES:** 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]

Wisconsin Administrative Code PI.9

**CROSS REFERENCES:**  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 and Guidelines;

Policy 361 – Instructional Resources

**POLICY ADOPTED:**  January 10, 2006

**POLICY REVISED:**  November 22, 2006, July 26, 2010, March 19, 2012,

August 25, 2014, December 2015, March 2016,

 August 26, 2019

Acceptable Use Agreement

Read and Signed by Student

I understand and will abide by the Acceptable Use Agreement. I further understand that any violation of these guidelines may result in my Internet privileges being restricted or revoked and also may result in school disciplinary action. If the violation constitutes a criminal offense, appropriate legal action may be taken.

Student’s Name (Please Print) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Student’s Signature \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Read and Signed by Parent/Guardian

As the parent or guardian of this student, I have read the Acceptable Use Agreement. I understand that this access is designed for educational purposes. I recognize that some controversial materials exist on the Internet. I will not hold the School District responsible for materials acquired on the network. I hereby give permission for my child to use the Internet at school.

Parent/Guardian’s Name (Please Print) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Parent/Guardian’s Signature \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Read and Signed by Employee or Authorized Guest

I understand and will abide by the Acceptable Use Agreement. I further understand that any violation of these guidelines may result in my Internet privileges being restricted or revoked and also may result in school disciplinary action. If the violation constitutes a criminal offense, appropriate legal action may be taken.

Employee’s/Guest Name (Please Print) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 Signature \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_