

SCHOOL DISTRICT OF WAUZKA-STEUBEN

INTERNET SAFETY AND ACCEPTABLE USE POLICY (AUP)

The School District of Wauzeka-Steuben provides Internet access from its network to students, Staff, and board members, and as such this policy is applicable to those groups.

Providing Internet access is an important part of preparing District students for the future. This goal includes the following objectives:

- Gain skills needed for the 21st century employment
- Provide access to global educational resources for class assignment
- Provide e-mail services to improve communication skills
- Provide access to enter learning partnerships to expand educational opportunities
- Improve the development and broadening of research skills
- Improve decision-making skills
- Develop higher levels of thinking
- Develop skills to differentiate and evaluate the value of resources

Students and parent(s)/legal guardian(s) should be aware that some materials available on the Internet could be objectionable, illegal, defamatory, inaccurate or potentially offensive to some people. While the District believes that the benefits to students from access to the Internet outweighs the risk of access to such material, parent(s)/legal guardian(s) are responsible for setting and conveying the standards that their child(ren) should follow when using media and information sources.

The District shares responsibility for control over access of inappropriate Internet materials. In light of that responsibility, the District utilizes hardware and software that is designed to filter and block inappropriate sites and high risk activities. The District reserves the right to block sites that do not enhance classroom activities. This filtering will, at a minimum, meet the requirements of the Children's Internet Protection Act (CIPA) to provide protection from obscene, pornographic, and other materials considered harmful to minors.

Children's Internet Protection Act Compliance

1. Parent(s)/Legal guardian(s) are responsible for setting and conveying standards that children should follow when using the internet.
2. A K-12 objective is to educate students on safety and appropriate use for online activities.
3. It shall be the responsibility of all members of the Wauzeka-Steuben School staff to supervise and monitor usage of the online computer network and access to the Internet in accordance with this policy and the Children's Internet protection Act.
4. Technology protection measures shall be used to block or filter access to inappropriate information on the Internet or through other forms of electronic communications.

The use of filtering hardware and software is not infallible. Objectionable material may be accessed notwithstanding our efforts to block such content. The use of an Internet filter does not diminish the user's personal responsibility to use the network in conformance with the standards in this policy.

Students and Staff are responsible for the ethical and educational use of their own Internet account. These accounts are to be used only by the authorized owner of the account for the authorized purposes.

Access to the network is a privilege, not a right. Procedures for disabling or otherwise modifying any technology protection measures shall be the responsibility of the school principal or his/her designee. 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.

The following activities are not permitted and will result in the immediate loss of Internet access, building level disciplinary actions, and may include expulsion/termination when discovered.

- Downloading, displaying, viewing, accessing or attempting to access, storing or transmitting any images, cartoons, messages, or materials which are obscene or sexually explicit;
- Downloading, displaying, viewing, accessing or attempting to access, storing or transmitting any images, cartoons, messages, or material that may be construed as threatening, harassing, offensive, or intimidating to others based upon gender, race, national origin, age, disability, religion, sexual orientation or any other basis protected by applicable law;
- Unreasonable personal use or personal use that interferes with an employee's or other district user's performance of his/her duties and/or responsibilities, or which otherwise disrupts the operations of the district;
- Use of the network for bullying, commercial, political, or advocacy purposes;
- Use which is illegal, including the violation of copyright or software licensing agreements, defamation, gambling and pornography laws;
- Damaging any component of the District's computer hardware or software; no deliberate attempts made to degrade or disrupt system performance, equipment, or software;
- Intentionally wasting limited resources including access time, paper, or occupying excessive file storage space and bandwidth;
- Unauthorized accessing or attempting to access confidential District information, including personnel records, medical records and financial information pertaining to the District or any of its employees or students;
- Unauthorized accessing or attempting to access an employee's or student's password, data, messages or other electronic communication materials

- Posting private information about a student or any other person, including but not limited to addresses, telephone numbers, identification numbers, account numbers, passwords, or access codes;

Violations may result in *any or all* of the following actions:

1. Parent/Legal guardian notification
2. Conference with an administrator/principal
3. Access restrictions
4. Revocation of network access
5. Other disciplinary action up to and including termination

The District's computer network is the sole property of the District. All electronic communications transmitted by, received from, or stored in the District's network are owned by the District. Students and Staff should have no expectation of privacy with regard to the use of the District's network or information, messages, files, and other data stored on these systems. The District may access, search, monitor and/or disclose to appropriate authorities any communication at any time without prior notice being given. Nothing residing in the network system or files or the District's e-mail system will be deemed personal, private, or confidential.

If a user inadvertently becomes connected to a site that contains any material with prohibited content, the user must disconnect from that site immediately and inform a staff member of the incident. A user is encouraged to inform a staff member if the student becomes aware that another user is accessing or has accessed prohibited material.

Students will be educated about appropriate online behavior, including interacting with others online (such as in social networking sites and/or chat rooms), appropriate communication with peers, and cyber bullying awareness and response.

Legal References: Wisconsin Statutes §§ Sections 120.13, 943.70, 947.0125; Children's Internet Protection Act

Cross References: Policies 347 Student Records, 771.1 Use of Copyrighted Materials

Adoption Date: 2/17/1998

Date Revised: 1/19/2009; 1/20/2014

Date Reviewed: