

STAFF INTERNET SAFETY & ACCEPTABLE USE

Policy #363.2 Rule 1

Page 1 of 4

Intent

The Waunakee Community School District will provide all staff access to technology resources including mobile devices and the Internet to support educational excellence in all our schools. The concept of internet safety and technology use has fundamentally changed and will continue to change in the future. It has become clear that safety is not just an exercise in protecting staff from online dangers or reducing risk for the district population; internet safety also means our staff are good digital citizens.

Staff should use the district's computer network in a way that is consistent with applicable district policies. Whoever uses the Waunakee Community School District computer network and other instructional technology is expected to behave ethically and to comply with District policy and administrative guidelines. Each employee is expected to understand and comply with the following rules and guidelines. Violation of the rules and guidelines in this policy will result in disciplinary action up to and including termination and legal action, if warranted.

Digital Citizenship

The Waunakee School District expects all users to demonstrate good digital citizenship. They are expected to:

1. Use digital tools, the network, and the internet appropriately for their position's needs.
2. Use only their own accounts.
3. Follow international copyright laws.
4. Be professional and courteous in their online communications as a representative of the district.
5. Treat all equipment with care.
6. Respect the work and privacy of others.
7. Keep passwords and login information private.
8. Alert an administrator if they receive or learn of threatening or inappropriate online communication, or activity.
9. Use only district authorized software and browsers.
10. Refrain from sharing personal information on the internet.
11. Record or take pictures of others only after obtaining their permission.
12. Remember that all network activities are monitored and retained.

Responsibility

Because the Internet is a network with global reach, individuals may encounter materials that are not considered appropriate or suitable by parents and other members of the learning community. Therefore, acceptable use behaviors and safety policies are outlined below. The District staff and parents and guardians are responsible for conveying and discussing responsible technology use with their students and children. In accordance with federal law, the staff is also responsible for monitoring student use of the Internet while in their classrooms. Although it is unlikely, individual users might gain access to inappropriate materials despite supervision and technology protection measures. Any observed intended, or unintended access to inappropriate material should be immediately reported to an administrator.

The individual user, student and staff alike, is ultimately accountable for all activities conducted while using the Internet, network, or other district instructional technology resources. The smooth operation of the computer network and Internet depends upon the proper conduct of the users. These guidelines are provided so that students and staff are aware of their responsibilities.

Terms and Conditions of Use

STAFF INTERNET SAFETY & ACCEPTABLE USE

Policy #363.2 Rule 1

Page 2 of 4

The following guidelines were written to correspond with federal and state law governing computerized communication systems (1995 Wisconsin Act 353, effective June 7, 1996, Children's Internet Protection Act, 2000).

1. Acceptable Use

- a. The Waunakee Community School District has established the computer network and other instructional technologies for a "limited educational purpose," which includes classroom activities, career development and teacher-approved self-discovery activities.
- b. The use of these resources must be in support of education and research and consistent with the educational objectives of the Waunakee Community School District.
- c. Transmission of any material in violation of any national or state regulation is prohibited. This includes, but is not limited to, copyrighted, harassing, threatening, or obscene material. Pirating, which is the illegal copying or selling of software or copyrighted material, is prohibited.
- d. Use any social media application with caution, please be aware that all social media related to staff may be subject to district policies regarding public records. Refrain from communication with students using social media.
- e. Staff may analyze legislative proceedings and matters of public concern and communicate with elected officials via the computer network. However, fund-raising for political activities may not be conducted using the network.
- f. The computer network is not for commercial purposes.
- ~~g.~~ Staff may not use the network to offer or provide products and services of a commercial nature.
- h. The District will comply with Wisconsin statutory requirements and administrative rules related to technology.

3. Technology Protection Measure

The term "technology protection measure" means a specific technology that blocks or filters Internet access to visual depictions that are:

- child pornography, as defined in Section 2256 of Title 18, United States Code; or
- harmful to minors.

a.- The Waunakee Community School District employs technology protection measures to protect students and other individual users from seeing inappropriate materials and prevent unauthorized individuals from gaining access to our network.

b. One of these technology protection measures shall be an Internet management application, or filter.

- The District shall filter websites that contain obscenity, child pornography, materials harmful to minors, and may filter sites that interfere with the educational objectives of the school or make excessive demands on network resources.
- The filter's database shall automatically download updates frequently to keep the protection as current as possible. The technical staff shall be able to open and close sites as needed for instructional purposes.
- Filtering shall be effective throughout the entire network.

c The District shall utilize firewall technologies to assist in preventing unauthorized access.

d The District has the capability to monitor Internet access and may check an individual's record of access.

5. E-mail and other electronic communication

a. All network users are expected to abide by the generally accepted rules of network etiquette. These include (but are not limited to) the following:

- Be polite. Do not write messages that will harass, offend, or insult anyone.
- Use appropriate language. Do not use profanity, sexual connotations, or other inappropriate language. Illegal activities are strictly forbidden.

- Users may not knowingly receive e-mail containing pornographic material or other inappropriate information and data. Please report all inappropriate materials to administration.
- Do not use the network in such a way that you would disrupt the use of the network by other users.
- Exercise caution if you receive an unexpected attachment. Contact the system administrator, a technician, or a lab assistant if you suspect a virus.
- E-mail attachments that you create or forward should be consistent with the educational mission of the school district.

b For your personal protection, do not give out your address or phone number.

c Note that e-mail and other electronic communication is not private, privileged, or confidential. People who operate the system have access to all mail. Messages relating to, or in support of illegal activities may be reported to the authorities.

d E-mail may be subject to district policies regarding public records.

6. Security

a. Security on any computer system is a high priority, especially when the system involves many users. If you feel you can identify a security problem on the network, you must notify a system administrator, technician, or lab assistant

b. Do not use another individual's account or password.

c. Attempts to logon to the network as a system administrator will result in cancellation of user privileges.

d. Any user identified as a security risk or having a history of problems with other computer systems may be restricted or denied network access.

7. Network Resources

a. Network resources, including but not limited to storage and connectivity, are limited. Avoid excessive demands on network resources.

b. Excessive demands on network resources are subject to restriction by the system administrator. Repeated excess demand on network resources will result in termination of access and possible administrative action.

8. Vandalism

a. Vandalism is defined as any malicious attempt to modify, damage or destroy data, software, operating systems, or equipment, or intentionally disrupt the system.

b. This includes, but is not limited to, the loading or creation of computer viruses and any attempt to bypass network security.

9. Consequences for Violations of the Acceptable Use Policy

a. Violation of any provision of the Acceptable Use Policy may lead to termination of access. School administrators will determine consequences for inappropriate use.

b. An administrator of the school may request the system manager to suspend specific staff user accounts until the incident is reviewed. The district may temporarily deny access to maintain network function or prevent a criminal act pending the disciplinary process.

c. Staff will receive notice of an alleged violation and an opportunity to respond before an extended termination of access.

d. First time violations of a minor nature may be addressed through administrative counseling.

e. Individuals may be subject to action under existing Board of Education Policies, school rules, and contractual agreements.

f. Termination of access does not prohibit the district from pursuing or implementing other disciplinary measures.

- Acceptable Use Violations that are severe or repeated may result in additional sanctions beyond termination of access up to, and including, staff dismissal.

STAFF INTERNET SAFETY & ACCEPTABLE USE

Policy #363.2 Rule 1

Page 4 of 4

- The district will contact appropriate local, state, or federal authorities if there is any suspicion of illegal activity. The District will lawfully cooperate with local, state, or federal officials in any investigation concerning illegal activities conducted through the District's network.

10. Privacy

- a. Files in individual, unshared, staff folders should not be viewed by other staff, with the exception of the system administrator, technical personnel, and supervisors.
- b. Files in shared folders are not private.
- c. Unauthorized disclosure, use, and dissemination of personal identification information regarding minors are prohibited. Communication with commercial website operators will be governed by the Children's Online Privacy Protection Act.
- d. The system administrator and technical personnel have the ability to access personal files, including e-mail.
- e. Regular network maintenance and monitoring may detect violations of the acceptable use policy.
- f. The system administrator and technical personnel will investigate unusual activity on the network and may access personal files in the course of such investigations.
- g. The district retains control of all data stored on all district-owned servers and devices and may exercise this control to monitor compliance with this policy.

11. Warranties of Service

- a. The Waunakee Community School District (WCSD) makes no warranties of any kind, whether expressed or implied, for the service it is providing.
- b. The WCSD will not be responsible for any damages you suffer. This includes loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions caused by its own negligence or your errors or omissions.
- c. The WCSD is not responsible for any costs, liabilities or damages caused by the way you use the computer network.
- d. Use of any information obtained via the Internet is at your own risk.
- e. The WCSD specifically denies any responsibility for the accuracy or quality of information obtained through its services.

Adoption Date: 1/10/96

Revised: 6/8/98
February 2002
February 2009
August 2018
May 2023