

**INTERNET SAFETY AND ACCEPTABLE USE POLICY
for Network Access
in the Waunakee Community School District**

365-Rule

Intent

The Waunakee Community School District is providing access to the Waunakee computer network and the Internet for teachers and students to promote educational excellence in schools by providing resource sharing, innovation, and communication.

The district has a paramount duty to provide education. Lifelong learning requires information gathering skills. Today, the acquisition of these skills demands the ability to access information electronically. Access to the Internet and other forms of instructional technology is an important learning resource.

The purpose of public education is to prepare students for life and work. In the world of work, students will encounter limited purpose networks. As part of the educational process, students should learn what conduct is appropriate on a limited purpose network versus what is appropriate on a personal account. 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.

The Waunakee Community School District has revised this policy in accordance with the Children's Internet Protection Act to comply with all federal requirements. This includes an Internet safety policy and a description of the technology protection measure in place. The district's student safety program will educate students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response. In addition, the policy addresses general network acceptable use.

The Internet is a global network connecting computers and individual subscribers throughout the world. In general, students and teachers will have access to:

- The World Wide Web.
- Information and news from various agencies as well as the opportunity to correspond with the scientists and other researchers at many institutions.
- Public domain software, graphics, and other media for school use.
- Storage of school related files.
- Libraries and informational databases.
- Electronic communication with people throughout the world (for class assignments).

Responsibility

Access to the Internet, district network, and other instructional technology is an important learning resource. The opportunity of access must be utilized responsibly to maintain a positive learning environment and instructional technology access for all. These technologies rely on convenient communication and shared resources. Therefore, individual users must be sensitive to the impact their actions may have on the learning community.

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.

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. If anyone violates any of these provisions, his/her account could be terminated, future access could be denied, and additional consequences imposed consistent with district policy, relevant codes, and agreements.

School Network, Internet, and Instructional Technology – Terms and Conditions of Use

The following policies 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
 - 1.1. 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.
 - 1.2. 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.
 - 1.3. 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.
 - 1.4. Pirating, which is the illegal copying or selling of software or copyrighted material, is prohibited.

- 1.5. Students and 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.
 - 1.5.1. Use by the Waunakee Teachers Association will be governed by the provisions of the collective bargaining agreement.
- 1.6. The computer network is not for commercial purposes.
 - 1.6.1. Students may not purchase products or services via the network without the permission of their principal.
 - 1.6.2. Staff may not use the network to offer or provide products and services of a commercial nature.
- 1.7. The District will comply with Wisconsin statutory requirements and administrative rules related to technology.

2. Technology Protection Measure

- 2.1. 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.
- 2.2. One of these technology protection measures shall be an Internet management application, or filter.
 - 2.2.1. 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.
 - 2.2.2. 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.
 - 2.2.3. Filtering shall be effective throughout the entire network.
- 2.3. The District shall utilize firewall technologies to assist in preventing unauthorized access.
- 2.4. The District has the capability to monitor Internet access and may check an individual's record of access.

3. Privileges

- 3.1. The use of the Internet is a privilege, not a right, and inappropriate use may result in a cancellation of those privileges.
- 3.2. The district provides information and training in proper use of the network. That instruction may include additional guidelines not mentioned in this policy.
- 3.3. Students may bring personal laptop and handheld computers or other devices to school under certain conditions and, in some instances, formal agreements.
 - 3.3.1. While the student's laptop, handheld computer, or other electronic device is at school, it is an instructional tool and must be used for school curriculum only. It may not be used as an entertainment system.
 - 3.3.2. The computer or other electronic device is to be used in compliance with the policies, rules, and regulations of the District. The Parent/Guardian and the Student will be bound by all policies and regulations of the District applicable to the use of instructional technology and access to the Internet. Any violation of such policies, rules and regulations may result in the exclusion of the device from school.

3.3.3. The District may examine computers and other electronic devices and search their contents, if there is a reason to believe that school policies, rules, or regulations have been violated. Individuals should have no expectation of privacy in the use of the district network.

4. E-mail and other electronic communication

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

4.1.1. Be polite. Do not write messages that will harass, offend, or insult anyone.

4.1.2. Use appropriate language. Do not use profanity, sexual connotations, or other inappropriate language. Illegal activities are strictly forbidden.

4.1.3. Users may not knowingly receive e-mail containing pornographic material or other inappropriate information and data. Please report all inappropriate materials to administration.

4.1.4. Do not use the network in such a way that you would disrupt the use of the network by other users.

4.1.5. Exercise caution if you receive an unexpected attachment. Contact the system administrator, a technician, or a lab assistant if you suspect a virus.

4.1.6. E-mail attachments that you create or forward should be consistent with the educational mission of the school district.

4.2. Electronic mail (e-mail) privileges or accounts may be given to students for specific assignments. Any e-mail, chat, or other direct electronic communication for instructional purposes will be closely supervised.

4.3. E-mail, chat, or instant messaging via the Waunakee School District Network is not to be used for the personal use of the student.

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

4.5. 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.

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

5. Security

5.1. 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. Students should report security issues to a building administrator, teacher, or lab assistant. Do not demonstrate the problem to other users.

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

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

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

6. Network Resources

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

- 6.2. Excessive demands on network resources are subject to restriction by the system administrator.
 - 6.3. Repeated excess demand on network resources will result in termination of access and possible administrative action.
7. Vandalism
- 7.1. Vandalism is defined as any malicious attempt to modify, damage or destroy data, software, operating systems, or equipment, or intentionally disrupt the system.
 - 7.2. This includes, but is not limited to, the loading or creation of computer viruses.
8. Consequences for Violations of the Acceptable Use Policy
- 8.1. Violation of any provision of the Acceptable Use Policy may lead to termination of access.
 - 8.2. School administrators will determine consequences for inappropriate use.
 - 8.3. An administrator, teacher, or other staff member of the school may request the system manager to suspend specific student 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.
 - 8.4. Students and staff will receive notice of an alleged violation and an opportunity to respond before an extended termination of access.
 - 8.5. First time violations of a minor nature may be addressed through teacher or administrative counseling.
 - 8.6. Individuals may be subject to action under existing Board of Education Policies, school rules, and contractual agreements.
 - 8.7. Termination of access does not prohibit the district from pursuing or implementing other disciplinary measures.
 - 8.7.1. Acceptable Use Violations that are severe or repeated may result in additional sanctions beyond termination of access up to, and including, expulsion (students) and dismissal (staff).
 - 8.7.2. 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.
9. Privacy
- 9.1. Files in individual, unshared, student folders should not be viewed by other students.
 - 9.2. Files in individual, unshared, staff folders should not be viewed by other staff, with the exception of the system administrator, technical personnel, and supervisors.
 - 9.3. Files in shared folders are not private.
 - 9.4. 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.
 - 9.5. The system administrator and technical personnel have the ability to access personal files, including e-mail.
 - 9.6. Regular network maintenance and monitoring may detect violations of the acceptable use policy.

- 9.7. The system administrator and technical personnel will investigate unusual activity on the network and may access personal files in the course of such investigations.
- 9.8. 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.
10. The Waunakee Community School District (WCSD) makes no warranties of any kind, whether expressed or implied, for the service it is providing.
 - 10.1. 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.
 - 10.2. The WCSD is not responsible for any costs, liabilities or damages caused by the way you use the computer network.
 - 10.3. Use of any information obtained via the Internet is at your own risk.
 - 10.4. The WCSD specifically denies any responsibility for the accuracy or quality of information obtained through its services.

Adopted: 1/10/96

Revised: 6/8/98
February 2002
February 2009

Waunakee Community School District