



Book	Policy Manual
Section	7000 Property
Title	INTERNET SAFETY AND RESPONSIBLE USE OF TECHNOLOGY FOR STUDENTS AND STAFF
Code	po7540.03
Status	Active
Adopted	November 7, 2017
Last Revised	May 20, 2025

7540.03 - **INTERNET SAFETY AND RESPONSIBLE USE OF TECHNOLOGY FOR STUDENTS AND STAFF**

This Internet Safety and Responsible Use of Technology Policy (RUP) includes sections covering:

- A. Introduction;
- B. Digital Citizenship;
- C. Examples of Unacceptable Use;
- D. Sanctions for Inappropriate Use;
- E. Internet Safety - Children's Internet Protection Act (CIPA) Compliance;
- F. Access to Inappropriate Material;
- G. Social Media;
- H. Education and Training;
- I. Definitions.

Introduction

This RUP provides use expectations of instructional and information technology at the Neenah Joint School District (NJSD). This RUP provides guidelines and direction for all student and staff users of District technology while on and off School District property. Students' use of District technology resources is an extension of school property with expectations and responsibilities for appropriate use and consequences for inappropriate use.

The NJSD Board of Education is committed to the effective use of technology to both enhance the quality of student learning and enhance the efficiency of operations. Technology resources that are owned and licensed by NJSD are the property of NJSD and are provided for students and staff to help achieve excellence in education. Technology includes but is not limited to computer systems, hardware and software, staff and student devices, Internet of Things devices, Internet access, e-mail, phone and voicemail systems, audio/video equipment, network infrastructure, servers, telecommunications, and related services. All authorized users will be issued user accounts and passwords, which they will be required to use. During regular school hours or when students and staff are on school grounds, all authorized users are expected to access Internet resources through their assigned NJSD network.

Because technology is ever-changing, this RUP provides a framework for building digital citizenship for staff and students, incorporating awareness of new ideas, understanding responsible use, and remaining flexible for the rapid changes in technology. It is the responsibility of all staff and students to ensure that NJSD digital resources are used responsibly.

Off-premises use of E-Rate-supported technology must be primarily for an educational purpose that is integral, immediate, and proximate to the education of students.

Digital Citizenship

Digital citizenship is the responsibility of all students and staff who access digital resources. When using District technology, students and staff are responsible for good behavior, just as they are in classrooms, school hallways, other school premises, and attending school-sponsored events. As noted in the introduction, technology includes but is not limited to Internet resources and devices listed above. This includes personal devices using NJSD network resources.

Digital activity is often public in nature. The Board only sanctions the use of technology that is authorized by, or conducted in compliance with, this RUP and its accompanying guidelines. Utilization of technology for non-school-related purposes may occur during personal time. All users must be aware that privacy is not, and cannot be, guaranteed. Furthermore, the District does not warrant network functionality and is not responsible for any information that may be lost, damaged, or become irretrievable when using the network. Likewise, the District does not guarantee the accuracy of information received.

Examples of Unacceptable Use

All students and staff are responsible for digital citizenship. Users are responsible for reporting occurrences of irresponsible or unacceptable use to school staff, administrators, or other school officials. It is impossible to completely define irresponsible or unacceptable use; however, for the purpose of illustration, examples include but are not limited to:

- A. Sending or displaying offensive messages or pictures;
- B. Using offensive or obscene language;
- C. Harassing, insulting, threatening, or attacking others, including racial or sexual slurs (i.e., cyberbullying);
- D. Damaging equipment or networks;
- E. Plagiarism or violation of copyright laws;
- F. Unauthorized access:
 - 1. Misrepresenting or masking identity;
 - 2. Intentional attempts to bypass filters;
 - 3. Using others' passwords;
 - 4. Accessing (logging on) to hardware assigned to others without their permission;
 - 5. Trespassing in others' folders, work, or files.
- G. Intentionally wasting resources:
 - 1. Excessive streaming of video for non-instructional/educational purposes;
 - 2. Denial of service attacks.
- H. Using District technology resources for personal commercial gain or to express political or religious views outside of the instructional process;
- I. Using the District email for personal communication purposes;
- J. Illegal activities;

K. Unauthorized installation of software;

L. The disclosure of Personally Identifiable Information (PII) about students online is prohibited. PII is any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. This includes, but is not limited to, any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Sanctions for Inappropriate Use of NJSD Technology

Technology administrators at the direction of NJSD administrators and/or their designee may review computer or school-assigned cloud-based files and communications to ensure that users are using systems responsibly to maintain system integrity and to comply with Wisconsin open records law. The Board reserves the right to access, inspect, review, monitor, and preserve any directories, files, and/or messages sent from or to, or residing on the District's computers, network, or other District-owned digital resources. Discipline measures may include, but are not limited to, the following:

- A. Discipline may be determined at the building and/or District level in line with existing practice regarding inappropriate behavior.
- B. Restrictions, including limited access or loss of access to the Internet, and/or loss or restrictions to user accounts and files.
- C. Restrictions on District-issued devices such as laptops, Chromebooks, or other hardware.
- D. Involvement of local, county, and/or state law enforcement agencies.

Internet Safety - Children's Internet Protection Act (CIPA) Compliance

This RUP is CIPA compliant (see Education Statute References below). It is the policy of NJSD to make a good-faith effort to:

- A. Prevent user (students, staff, minors, adults) access over the District computer network to view or transmit inappropriate material via the Internet, electronic mail, video, or other forms of direct electronic communication.
- B. Prevent unauthorized access, including hacking, and other unlawful online activity.
- C. Prevent unauthorized online disclosure, use, or dissemination of personal identifiable information of minors.

Access to Inappropriate Material

To the extent practical, technology protection measures (e.g., "Internet filters") shall be used to block and/or filter access to inappropriate Internet sites and information. Specifically, as required by CIPA, blocking shall be applied to visual depictions of material deemed obscene or to be child pornography, or to any other material deemed harmful or age-inappropriate to minors. Subject to staff supervision and administrative approval, technology protection measures may be adjusted for bona fide research or other lawful purposes. Procedures for any disabling or otherwise modifying technology filtering measures shall be the responsibility of the Director of Instructional Technology or their designee.

Realizing that no Internet filtering device is 100% effective, NJSD shall make reasonable efforts to maintain and update effective content filtering hardware and software. 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 unintended 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, parent, or citizen is encouraged to contact a building or District Administrator with a concern. If the issue is not resolved, they can contact the Federal Communications Commission (FCC). To the extent practical, steps shall be taken to promote the safety and security of users of the NJSD computer network when using electronic mail, social media, instant messaging, video, and other forms of direct electronic communications (whether use is intended or accidental). During regular school hours or when students and staff are on school grounds, all authorized users are expected to access Internet resources through their assigned NJSD network.

Internet filtering software is in use for student-assigned digital devices when accessing Internet resources on school grounds. Student devices will also be filtered for content at home or off campus. However, NJSD is not responsible for students' use of proxy websites to bypass filtering when used through home networks. Personal, public, or commercial

Internet providers available in the community may allow access to sites that are blocked at school. The Parent/Guardian and student are solely responsible for following this RUP when accessing Internet resources away from school through home or community Internet connections.

Social Media

Webster's Dictionary defines social media as: "forms of electronic communication (such as websites for social networking) through which users create online communities to share information, ideas, personal messages, etc." Examples include, but are not limited to, Facebook, Instagram, Snapchat, Twitter, etc.

An employee's use of social media may have unintended consequences. Use of social media should occur in a manner sensitive to the employee's professional role and responsibilities, and staff should maintain an appropriate professional relationship with students. Access to social media, blogs, or chat rooms for personal purposes from the District's network by staff is expressly prohibited during instructional time. Staff shall be granted access to social media through District hardware, network, or other resources for educational purposes at any time.

Staff will be assigned a school email address that they are required to utilize for all school-related electronic communications, including those to students, parents, and other constituents, fellow staff members, vendors, or individuals seeking to do business with the District.

Student use of technology resources, including accessing social networks at school, shall be in accordance with all provisions of this RUP within school grounds or during school-sanctioned events. Students shall not access social media for personal use from the District's computers, network, or other resources. However, students may be permitted access to social media for educational use in accordance with their teacher, coach, or faculty advisor's plan, approved by their building administrator.

Education and Training

NJSD will educate staff annually about responsible digital behavior. All instructional members of NJSD staff are responsible to learn about, educating students, supervising student use, and monitoring appropriate and responsible use of the NJSD computer network. Staff shall access the Internet in accordance with this RUP. All instructional members will be knowledgeable of the Children's Online Privacy and Protection Act (COPPA), Family Education Rights and Privacy Act (FERPA), and the Protecting Children in the 21st Century Act. During Instructional time, staff use of technology is for teaching and learning purposes only. All NJSD staff will receive annual training related to this RUP and other technology issues. Training will be administered by the Instructional Technology Department.

NJSD Instructional Technology Department will educate students annually about responsible digital behavior. Annual instruction of students will include, but not be limited to:

- A. The RUP is an age-appropriate lesson;
- B. How to locate and evaluate appropriate digital sources;
- C. Information literacy skills, including understanding of safety, copyright, ethical practice, and data privacy;
- D. Proper safety procedures when using electronic communication;
- E. Consequences of inappropriate use.

Definitions

Key terms as defined by CIPA

A. 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;
3. Harmful to minors as defined to mean any picture, image, graphic image file, or other visual depiction that:

- a. Taken as a whole and 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 a lewd exhibition of the genitals;
- c. Taken as a whole, lacks serious literary, artistic, political, or scientific value for minors.

B. Sexual Act; Sexual Contact

The terms "sexual act" and "sexual contact" have the meanings given to such terms in section 2246 of title 18, United States Code.

NJSD Policy References:

NJSD School Board Policies, including but not limited to:

3362 - Employee Anti-Harassment
4122.02 - Non-Discrimination Based on Genetic Information of the Employee
4362 - Employee Anti-Harassment
5505 - Academic Honesty
5500.01 - Conduct in a Virtual Classroom
5136 - Wireless Communication Devices
5517 - Student Anti-Harassment
5517.01 - Anti-Bullying

State of Wisconsin Legal Reference Sections:

The following State of Wisconsin Statutes provide more details about situations where law enforcement could be involved in student or staff unacceptable use of NJSD digital resources.

943.70. Computer Crimes
947.0125. Unlawful Use of Computerized Communication Systems
118.325. General School Operations, Locker Searches
120.13(1). School Government Rules: Suspension; Expulsion

Revised 9/20/22
Revised 3/19/24
Revised 12/17/24

© Neenah Joint School District 2024