INTERNET SAFETY AND RESPONSIBLE USE OF TECHNOLOGY POLICY

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

- Introduction
- Digital Citizenship
- Examples of Unacceptable Use
- Sanctions for Inappropriate Use
- Internet Safety - Children's Internet Protection Act (CIPA) Compliance
- Access to Inappropriate Material
- Social Media
- Education and Training
- Definitions

Introduction

This RUP replaces the existing Acceptable Use Policy (AUP) and 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 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 remains flexible for the rapid changes in technology. It is the responsibility of all staff and students to assure that NJSD digital resources are used responsibly.

Digital Citizenship

Digital citizenship is the responsibility of all students and staff that 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 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:

- Sending or displaying offensive messages or pictures
- Using offensive or obscene language
- Harassing, insulting, threatening or attacking others, including racial or sexual slurs (i.e. cyberbullying)
- Damaging equipment or networks
- Plagiarism or violation of copyright laws
- Unauthorized access
    - Misrepresenting or masking identity
    - Intentional attempts to bypass filters
    - Using others' passwords
    - Accessing (logging on) to hardware assigned to others without their permission
    - Trespassing in others' folders, work or files
- Intentionally wasting resources
    - Excessive streaming of video for non-instructional/education purposes
    - Denial of service attacks
- Using District technology resources for personal commercial gain or to express political or religious views outside of the instructional process
- Illegal activities
- Unauthorized installation of software

Sanctions for Inappropriate Use of NJSD Technology

Technology administrators may review computer or school assigned cloud-based files and communications to ensure that users are using systems responsibly and 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:

- May be determined at the building and/or District level in line with existing practice regarding inappropriate behavior.
- Violations may result in usage restriction, including limited access or loss of access to the Internet, and/or loss or restrictions to user accounts and files, 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:

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

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.

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, educate, supervise and monitor 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 Team.

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

- How to locate and evaluate appropriate digital sources
- Information literacy skills, including understanding of safety, copyright, ethical practice and data privacy
- Proper safety procedures when using electronic communication

Definitions - Key terms as defined by CIPA

1. Technology Protection Measure

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

- Obscene: as that term is defined in section 1460 of title 18, United States Code
- Child pornography: as that term is defined in section 2256 of title 18, United States Code
- Harmful to minors defined to mean any picture, image, graphic image file, or other visual depiction that:
- Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
- 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;
- Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

2. 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.

NJSD Policy References:

NJSD School Board Policies 3362, 4122.02, 4362, 5136, 5517, 5517.1

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

Education Statute References

- Children's Internet Protection Act Public Law (CIPA) 106-554 and 47 USC 254(h)(5)(b)
- Children's Online Privacy and Protection Act (COPPA) 16 CFR Part 312 15 U.S.C. 6501–650
- The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)
- Protecting Children in the 21st Century Act – Pub. L. No. 110-385 Title II

NJSD School Board approved: 11/07/2017