SCHOOL DISTRICT OF THE MENOMONIE AREA

527-Rule

STAFF RULES FOR ACCEPTABLE USE OF DISTRICT TECHNOLOGY
AND ELECTRONIC COMMUNICATION RESOURCES

Staff in the School District of the Menomonie Area may have access to a variety of information technology, electronic communications, and social media resources. This use is a privilege and staff having access to these resources shall adhere to the following guidelines.

1. General
    a. All employees are required to sign a "Technology Use Policy Agreement" upon being hired. This form will be included in staff members' personnel files. Failure to sign this agreement does not exempt the staff member from compliance and may result in the loss of access privileges.
    b. The district's technology systems are provided on an "as is, as available" basis. The district does not make any warranties, whether expressed or implied, including, without limitation, those of merchantability and fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein.
    The district does not warrant that the functions or services performed by, or that the information or software contained on the system will meet the system user's requirements, or that the system will be uninterrupted or error-free, or that defects will be corrected. Opinions, advice, services, and all other information expressed by system users, information providers, service providers, or other third-party individuals in the systems are those of the individual or entity and not the district. The district will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the district's technology systems, including electronic communication resources.

2. User Responsibilities
    a. Users are responsible for individual accounts assigned to them and should take reasonable precautions to prevent others from accessing their accounts. Under no circumstances should users provide their passwords to another person. If a staff member compromises his or her account security, the district may require that 2-step authentication is enabled on the staff member's account. Users will contact the Technology Services department immediately if they identify a possible security problem. Users will not search for security risks as this may be construed as an unauthorized attempt to gain access to accounts or systems (hacking).
    b. All employees have access to a Google cloud-based drive on which to store data. It is the responsibility of the user to practice file management, using network and/or cloud-based storage.
    c. Staff members are expected to use District technology systems in an appropriate manner and will not engage in any of the following conduct:
        - Users may not use the District's technology systems for commercial purposes, including, but not limited to, purchasing, selling or advertising goods or services.
        - Online gambling is not allowed.
        - Users will not use obscene, profane, vulgar, rude, inflammatory, threatening or disrespectful language.
        - Users will not engage in personal attacks, such as, prejudicial or discriminatory attacks.
        - Users will not engage in cyberbullying, harassment, or posting false or

defamatory information about a person or organization. Staff members shall immediately disclose to their supervisor or Human Resources any electronic communications that are inappropriate or that make them feel uncomfortable.

- Users will not use district technology systems to access, view, store, or transmit material that is commonly considered offensive, including, but not limited to, hate mail, discriminatory remarks and/or materials, and obscene or pornographic material. If a staff member inadvertently accesses or receives inappropriate material through electronic communication (e.g. email), he or she should immediately disclose the incident to his or her supervisor. Reporting inadvertent access protects users against allegations that they have intentionally violated district policy and rules.
- Users will not attempt to gain unauthorized access to the district's technology systems or to any other computer system through the district technology systems, or go beyond their authorized access. This includes attempting to log in through another person's account or access another person's files.
- Users will not make deliberate attempts to disrupt the district's technology systems' performance or destroy data by intentionally spreading computer viruses or by any other means.
- Users may not plagiarize, copy or redistribute copyrighted programs or data without the written permission of the copyright holder or designee.This includes not using Artificial Intelligence (AI) to replicate or modify copyrighted materials without permission and citing all sources of content, including AI generated content, to avoid plagiarism.
- Users will not access or share confidential student, personnel or other district records without authorization. Any access to or disclosure of confidential student information must comply with state and federal laws governing the confidentiality of student records and the district's student records policy. This extends to the use of Artificial Intelligence (AI) tools where personally identifiable, confidential, and/or sensitive information should never be shared unless such sharing is explicitly approved by the district. Beyond student records, confidential records include, but are not limited to, evaluations, credit card numbers, private contact information, and health information.
- Users will not use district technology resources to engage in or support any illegal activity or violate any other district policies or local, state, or federal law.

3. Instructional Technology Use
    a. The district encourages the use of web resources and applications to enhance and extend student learning.
    b. Web resources and applications that are used by students and/or collect student data need to be pre-approved by the district. The approval process ensures these tools have a Family Educational Rights and Privacy Act (FERPA) compliant privacy policy and comply with the Children's Online Privacy Protection Act (COPPA) requirements and the Children's Internet Protection Act (CIPA).

4. Electronic Communications
    a. Electronic communications are protected by the same laws and policies and are subject to the same limitations as other types of district communication. The district expects staff to adhere to state and federal laws, as well as district policies and rules, when creating, using, or storing messages on the network. Staff should use added caution when committing confidential information to electronic messages, as confidentiality cannot be guaranteed.
    b. Because all technology systems, including all computer hardware, electronic

communication devices and software belong to the district, users have no reasonable expectation of privacy, including the use of email, text messages, and other forms of electronic communications, e.g. voicemail, Twitter™, Facebook ™, etc. except as noted herein. Users also have no expectation of privacy in any of the websites that they may visit by using the district's technology systems. In the process of monitoring and filtering, the district may inadvertently obtain access information for a staff member's personal internet account through the use an electronic device or program that monitors the district's network or through an electronic communications device supplied or paid for in whole or in part by the district. If such personal internet access is information is obtained by the district, the district shall not use that access information to access the staff member's personal internet account unless permitted by law.

c. Retention of Electronic Communications: The District archives all non-spam emails sent and/or received on the system in accordance with the District's adopted record retention schedule. After the set time has elapsed, email communications may be discarded unless the records may be relevant to any pending litigation, pending public records request, or other good cause exists for retaining email records.

5. Electronic Recordings
   Employees shall not electronically record by audio, video, or other means, any conversations or meetings unless each and every person present has been notified and consents to being electronically recorded. Persons wishing to record a meeting must obtain consent from anyone arriving late to any such meeting. Employees shall not electronically record telephone conversations unless all persons participating in the telephone conversation have consented to be electronically recorded. These provisions are not intended to limit or restrict electronic recording of publicly posted School Board meetings, grievance hearings, and any other Board-sanctioned meeting recorded in accordance with district policy. These provisions are not intended to limit or restrict electronic recordings involving authorized investigations conducted by district personnel, or authorized agents of the district, or electronic recordings that are authorized by the district, e.g. surveillance videos, extracurricular activities, voicemail recordings.

6. Personally-Owned Devices
   a. The district offers guest wireless access in each building. All users agree to the following terms when connecting to the district network:
      - Users will have current anti-virus software installed and updated on their devices before connecting.
      - Users will follow all appropriate district policies and rules, including but not limited to acceptable technology use.
      - The district is not responsible for any damage that may occur as a result of connecting to the wireless network.

   b. Personal electronic devices may only be connected to the Internet through the district's filtered guest wireless network. Users may connect personal devices to non-networked equipment such as a projector or Smartboard for educational purposes with the permission of a staff member. Personally-owned devices are not permitted to access district printers or copiers.
   c. Any personally-owned device brought to school is to be used in compliance with district policies and rules, including but not necessarily limited to those applicable to the use of district technology and electronic communications. Any violation of such policies or rules may result in the exclusion of the device from school and/or discipline of the person who has violated the policy and/or rule.
   d. If a personally-owned electronic device, such as a cell phone, is found or confiscated, the person recovering the device is not permitted to view the contents of the device. Lost devices will be turned into the office.
   e. The district may only search personally-owned computers and communication devices

if there is reason to believe that the owner violated school policies, rules, or laws. The search is limited to the specific violation and will be conducted according to legal requirements. There is no expectation of privacy in the use of the district's wireless network or technology systems and all such use is subject to monitoring.

f. The district does not require staff to bring personally-owned electronic devices to school. The district will not be responsible for the loss, theft, or damage of personal property brought to school. Any personal device brought to school is the responsibility of the owner.

7. Violations
    a. The district will cooperate fully with local, state, or federal officials in any investigation concerning or relating to any illegal activities conducted through district technology resources.
    b. Staff violations of the district's use of technology and electronic communications policy and/or rules will be investigated and handled in accordance with district policies and the Employee handbook.

Adopted:July 22, 2024

STAFF RULES FOR ACCEPTABLE USE OF DISTRICT TECHNOLOGY
AND ELECTRONIC COMMUNICATION RESOURCES

RETURN THIS FORM TO HUMAN RESOURCES DEPARTMENT

I have read this agreement and understand that the intent of the Staff Rules for Acceptable Use of District Technology and Electronic Communication Resources is to insure that staff use of technology and communication resources (e.g. hardware, software, internet, email) in this school district are for educational purposes. I further understand that the district and/or its designee reserves the right to monitor all e-mail, network, system, and internet related activities of the staff member, and that such activities are considered to be public (not private) communications.

While the district has undertaken steps to restrict access to controversial material, it is not possible for the district to restrict access to all controversial material and I will not hold the district responsible for material acquired on email, the network, and/or the Internet.

I understand that a violation of these provisions may result in the staff member losing access to email, the network, systems, and/or the Internet and possible legal or disciplinary action on the part of the district or by the appropriate law enforcement agency.

_____ _____ _____

User Name (print, including middle initial) Building Staff ID Number (if available)

_____ _____

User's signature Date