POLICY 4226
STAFF TECHNOLOGY ACCEPTABLE USE POLICY

Technology may be used for instruction, research, communication and other educational or professional purposes. Employee use of technology shall be consistent with the educational goals and objectives of the District and shall comply with applicable Board policies and rules.

The District will maintain a District website and use social media for the purpose of collaborating, communicating and disseminating District information. Content posted on the District's website and social media pages is the property of the District.

The District's electronic communication system, which includes telephones, copy/scan/fax machines, desktop computers, laptop computers, mobile devices, email and the network, is the property of the District. All messages, information and data sent, received or stored on the District's electronic communication system is the property of the District. The District reserves the right to monitor employee and student use of technology and inspect any messages, information or data sent, received or stored on the District's electronic communication system.

Failure to comply with this policy and its implementing rule may result in discipline, up to and including termination.

LEGAL REF
Wis. Stat. § 118.001[Duties and powers of school boards]
Wis. Stat. § 120.12 School board duties
Wis. Stat. § 120.13 School board powers
Wis. Stat. § 943.70 Computer crimes
Wis. Stat. § 947.0125 Unlawful use of computerized communication systems
Wis. Stat. §§ 19.31 - 19.39 Declaration of policy
Wis. Stat. § 115.31 License or permit revocation; reports; investigation
Wis. Stat. §§ 19.62 - 19.80 Definitions
Children's Internet Protection Act
Neighborhood Children's Internet Protection Act
Children's Online Privacy Protection Act

CROSS REF
1210 Communicating with Parents/Guardians
1240 Access to Public Records
1510 Advertising/Promotions
3531.1 Copyrighted Materials
4111 Employee Harassment
4224 Employee Code of Ethics
4260 Personnel Records
4362 Employee Discipline
6100 Mission, Vision, Core Values and Strategic Goals

6470 Student Records
6633 Student Technology Acceptable Use Policy
Employee Handbook

AFFIRMED July 20, 2010

REVISED March 22, 2016
September 24, 2019
October 27, 2020

RULE 4226
GUIDELINES FOR STAFF TECHNOLOGY ACCEPTABLE USE

For the purposes of this document, an electronic communications system is defined as the District's technology offerings, including but not limited to telephones, mobile phones, fax/scan/copy machines, Internet, Wi-Fi, the network computing devices and other technology tools available to staff.

1. Responsibility: Employees are responsible for the proper use of any District electronic communication accounts that are issued under their name or that the employee is charged with managing. Employees are responsible for ensuring proper use of technology by students under their supervision. Responsible use of the Internet includes such items as abiding by copyright laws and terms and condition policies. Understanding unethical and unlawful activities include unauthorized access to any data or communications equipment, "hacking", or unauthorized disclosure, use, or dissemination of anyone's personal information. The administration shall take steps to ensure that instruction or training activities and reasonable structural and systemic supports are in place to facilitate and enforce individual user's compliance with the District's policies, rules, and procedures that govern the acceptable, safe, and responsible use of the District's technology-related resources. All staff are to relinquish any and all KUSD owned devices upon separation from KUSD employment. Any shared media (i.e. Google files) that are the product of employment should have ownership and rights transferred to an assigned KUSD staff member prior to separation.

2. Passwords and security: All KUSD staff are expected to protect and update their electronic access and credentials. All users that have access to District technology resources must comply with the following rules for maintaining and securing District property and resources.
    - KUSD utilizes an email security campaign for educating staff with periodic phishing simulations and training resources. Staff that demonstrate a repeated concern from these tests will receive additional support and education.
    - Employees are prohibited from sharing their password for any electronic communication accounts that are issued under their name. Employees may, however, share their password with a member of the IT staff if necessary. In that case, the employee shall change his or her password immediately after the IT staff member has completed all support.
    - Employees must maintain a password for accounts and change passwords periodically as directed by the District.
    - Any computer or similar device should be secured whenever it is not in use by invoking the password on the computer and/or logging off the device. Leaving a computer open or logged in while away enables others to potentially access e-mail and other sensitive files; and All District technology should be physically secured according to standards set by building administrators or their designees when not in use.

- Employees are prohibited from accessing another user's account without permission. If an employee identifies a security problem associated with the network or his or her user account, the employee shall notify IT staff.

3. Privacy: All KUSD user accounts are owned by KUSD and therefore are not private. Passwords are for the purpose of preventing unauthorized access to the District's electronic communication system only; employees have no expectation of privacy when using the District's electronic communication system, even for personal use. The electronic communication system is the property of the District, and the District reserves the right to monitor and inspect any messages, information and data sent, received or stored on the District's electronic communication system. Documents or messages created, sent, received or stored on the District's electronic information system may be considered a public record and subject to disclosure under the Public Records Law. The administration may access any message for reasons including, but not limited to:
   - finding lost messages;
   - assisting employees in their performance of job duties;
   - studying the effectiveness of the communication system;
   - complying with investigations into suspected criminal acts or violation of Board policies or work rules;
   - recovering from systems failures and other emergencies;
   - complying with discovery proceedings or to be used as evidence in legal actions; and/or may otherwise be required or permitted by state or federal law

4. Prohibited use of the District's electronic communication system: Employees' use of the District's Electronic Communication System must reflect the District's standards for professionalism. The district's computer network and Internet system do not serve as a public access service or a public forum. Employees shall not use the District's electronic communication system for:

   - Accessing, sending, viewing or storing messages, images, websites or other materials which are sexually explicit, obscene, pornographic, or harmful to minors;
   - Soliciting for personal commercial activities or non-District related organizations or activities, unless approved by the District pursuant to the procedures in Board Policy 1500;
   - Accessing or disclosing confidential information without authorization. Any access to or disclosure of confidential student information must comply with the Family Educational Rights and Privacy Act, Section 118.125 of the Wisconsin statutes and the District's student records policy; or
   - Any other purpose which would violate law or Board policy (including harassment policies).

5. Use of District technology equipment off District premises: Employees may use District-owned technology equipment off District premises with appropriate administrator approval. Technology equipment may not be removed from a District building if its removal in any way causes disruption to the learning environment or decreases access to technology for District staff. Any technology assigned to staff for both on and off premises must be reflected in the KUSD Asset Manager system. A virtual private network (VPN) solution allows staff to work on their district assigned device outside of the KUSD network. This scenario ensures proper security and access to internal resources for job responsibilities. Staff that utilize a VPN will be filtered and protected as if they were physically operating behind the KUSD firewall.

   Employees who use District equipment off District premises will accept full and unconditional responsibility for any equipment damage or loss and will reimburse the District within a reasonable time for the applicable repair/replacement cost. Further, the responsible party agrees to hold the District harmless for damages caused to any individual or others by the use of this equipment.

6. Personal use of the District's electronic communication system: Incidental and occasional personal use of the District's electronic communication system is permitted, but such use is subject to this policy. Personal use of technology must be limited to break time and time outside the work day. Personal use must not interfere with student instruction, the performance of an employee's job duties or District business. Employees shall not use their District email address for personal commercial purposes. The District is not responsible for the safety or security of personal technology devices or the software on them that employees choose to bring into the District. The District does not provide technology support for personal devices.

7. Personal/off-duty use of social media and personal Web pages: Even if an employee is off-duty and not using the District's electronic communication system, an employee's personal use of technology or social media may be subject to this policy and regulated by the District if: the employee chooses to identify himself/herself as a District employee; the use affects the employee's job performance or the performance of other District employees or the use involves or relates to the District, District students/families or District employees. Unless authorized to do so by the superintendent or his/her designee, employees shall not: represent themselves as a spokesperson for the District or create or post content to a personal/non-authorized website that purports to be an official/authorized website of the District. Employees shall not use their District email address to register for a personal social media account and shall not post photos of students or other personally identifiable confidential student information on personal pages and/or sites without the written consent of the adult student or the minor student's parent/guardian.

8. Electronic communication with students: Employees shall use their District email address when communicating with students. Unless authorized to do so by the superintendent or his/her designee, employees shall not communicate with students via their personal email addresses, social media accounts, home phones, cellphones or other application not authorized by the District for communication with students. Employees also should use discretion when communicating with parents on social media (e.g., accepting "friend" or "follower" requests). Staff have KUSD approved communication options for authorized use. Staff provided email and resources should be used as the communication portal for interacting virtually with students. Guidance, training and support for currently available technologies and future utilities will be shared and integrated when possible.

9. Personally identifiable information relating to individual students or their families, except as permitted by the Family Educational Rights and Privacy Act, Section 118.125 of the Wisconsin statutes, and the District's student records policy. Elementary (4K-5) students only may be identified by their first name and last initial. Note: Regardless of age, photos, videos, names, artwork or other likenesses cannot be used if a student has a media restriction on file. Home telephone numbers, home addresses and email addresses of students and their family members shall not be posted or shared.

10. The District's website/social media pages: The superintendent or his/her designee reserve the right to approve content posted on the District's website and social media pages. All school-level Web editors must communicate with the District Web Specialist for information and assistance. The editors are responsible for ensuring accurate information is shared by maintaining the website and requesting updates be made by the Web specialist. The social media administrators are responsible for ensuring accurate and timely information is shared/posted. The Web editors and social media administrators are expected to ensure accurate spelling and grammar.

    The following content shall not be posted or shared on the District's website or social media pages:

    - Content that is sexually explicit, obscene, pornographic or depicts alcohol, drug or tobacco use.
    - Copyrighted material without the written consent from the owner and proper attribution.
    - Any photos, videos, names, artwork or other likenesses of students with a media restriction on file.
    - Links to personal or commercial websites.
    - Content that violates Board policy or rules.

11. The staff directed use of digital applications: Educators need to be aware of how data privacy, confidentiality and security practices affect students. When engaging with online educational service providers, educators must review the privacy policies prior to having students create accounts in selected applications. The Children's Online Privacy Protection Act (COPPA) governs online collection of personal information from children under age 13. Educators can act in the capacity of a parent to provide consent to sign students up for online education programs that are COPPA compliant at the school for the use and benefit of the school, and for no other commercial purpose.