MIDDLETON-CROSS PLAINS AREA SCHOOL DISTRICT

Administrative Policy and Procedure Manual

522.7

DISTRICT ACCEPTABLE USE FOR INTERNET AND ELECTRONIC MEDIA/DEVICES FOR STAFF

Policy

This policy is to set forth guidelines for access to acceptable and safe use of the District's electronic technologies and digital communication devices for staff. The District is committed to providing technology resources that allow employees, students, parents and community to communicate effectively.

Procedure

Access to technology in the Middleton-Cross Plains Area School District has been established for educational purposes. The use of the electronic technologies is a valued resource to our community. All electronic technologies must be used in support of the educational program of the District.

1. **Electronic Communications**

   Electronic communications are protected by the same laws and policies and are subject to the same limitations as other types of media. When creating, using or storing messages on the network or a district provided digital communication device, the user should consider both the personal ramifications and the impact on the District should the messages be disclosed or released to other parties. Extreme caution should be used when committing confidential information to the electronic messages, as confidentiality cannot be guaranteed.

   The District may review email logs and/or messages at its discretion. Because all computer hardware, digital communication devices and software belong to the District, users have no reasonable expectation of privacy, including the use of email, text-message and other forms of digital communications, such as social media, etc. except as noted herein. The District may through such review of email logs and/or messages inadvertently obtain access information for an employee's or student's personal internet account through the use of 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 employer. If such personal internet access information is obtained by the District, the District shall not use that access information to access the employee's or student's personal internet account unless permitted by law.

   Electronic mail transmissions and other use of the District's electronic communications systems or devices shall not be considered confidential and may be monitored at any time by designated District staff to ensure appropriate use. This monitoring may include, but is not limited by enumeration to, activity logging, virus scanning, and content scanning. Participation in computer-mediated conversation/discussion forums for instructional purposes must be approved by the Assistant Superintendent of Educational Services or his/her designee. External electronic storage devices are subject to monitoring if used with District resources.

   The use of District's technology, electronic resources and digital communication devices are an expectation of employment. Depending on the nature and degree of the violation and the number of previous violations, unacceptable use of electronic technologies may result in one or more of the following consequences: suspension or cancellation of use or access privileges; payments for damages and repairs; discipline under other appropriate District policies, including suspension, exclusion or termination of employment; or civil or criminal liability under other applicable laws.

2. **User Responsibilities**
District employees are responsible for their actions in accessing available electronic resources. The following standards will apply to all users (students and employees) of the Network, Internet, or District provided digital communication device, e.g. smartphone, tablet, etc.:

    a. The employee in whose name a system account is issued or a digital communication device is provided will be responsible at all times for its proper use. Employees may not access another person's account or use another person's digital communication device without written permission from an administrator or immediate supervisor.
    b. Each employee is responsible for his or her password security. An employee may not share their password with a student under any circumstances. Password security is the responsibility of each employee and may not be shared with other employees, unless sharing is approved by their supervisor in writing for a specific, stated reason.
    c. The system issued or a District provided digital communication device may not be used for illegal purposes, in support of illegal activities, or for any other activity prohibited by District policy.
    d. Users may not redistribute copyrighted programs or data without the written permission of the copyright holder or designee. Such permission must be specified in the document or must be obtained directly from the copyright holder or designee in accordance with applicable copyright laws, District policy, and administrative regulations.
    e. A user may not disable Internet tracking software or implement a private browsing feature on District computers, digital communication devices or networks. Browsing history shall only be deleted by authorized staff or in accordance with the District's technology department's directives.

3. **Unacceptable Uses**
Employees are responsible for anything ~~set~~ sent on the network or stored on their District provided electronic device(s) with their name or other individually identifiable information, e.g., IP address on it. Employees shall not engage in any activity that disrupts or hinders the performance of the District's electronic technologies.

    Users will not use the District's electronic technologies for political campaigning, personal businesses or profit generating purposes.

    Users will not use the District's electronic technologies to access, review, upload, download, store, print, post, receive, transmit or distribute:

    a. Pornographic, obscene or sexually explicit material or other visual depictions that are harmful;
    b. Obscene, abusive, profane, lewd, vulgar, rude, inflammatory, libelous, threatening, disrespectful, or sexually explicit language;
    c. Materials that use language or images that advocate violence or discrimination toward other people (hate literature) or that may constitute harassment or discrimination, or any other material that would violate any law.
    d. Any content that is disruptive to the educational environment or process.

    If a user accidentally reaches such material, the user must immediately back out of the area on the Internet containing educationally inappropriate material. The user must then notify the building

administrator and/or immediate supervisor of the site address that should be added to the filtering software, so that it can be removed from accessibility.

4. **Personal End User Devices**

    a. Personal end-user devices (e.g. laptops, tablets, smart phones, etc.) are not managed or supported by the District. Employees are solely responsible for any personal device that they bring on District property. When employees are on contract time or in District facilities; however, the same standards outlined in Section 3 apply.
    b. Personal devices may only be connected to the District's wireless access and never physically plugged into a network drop.
    c. Users of personal devices, when on district property or engaged in school related activities, are expected to adhere to the standards in Section 3, regardless of the network they are connected to, including non-district networks.

5. **Electronic Communications with Students**

"Communicate" in the context of this policy means to convey information directly and includes a one-way communication, as well as, a dialogue between two or more people. A public communication by an employee that is not targeted at students (e.g., a posting on the employee's personal social network page or a blog) is not considered communication; however, the employee may be subject to District regulations on personal electronic communications. Unsolicited contact from a student through electronic means is not a communication.

"Electronic media" includes all forms of social media, any form of texting, chat, or video/audio conferencing.

These regulations do not refer to students with whom the employee has a preexisting social or family relationship.

    a. Employees should only communicate electronically with students for which they have an instructional, supervisory or safety check responsibilities. The employee shall limit communications to matters within the scope of the employee's professional responsibilities. For classroom teachers, this refers to matters relating to class work, homework and tests or for coaches and trainers, this refers to matters related to extra-curricular purposes.
    b. The employee is prohibited from communicating with students through a personal social network page; the employee must create a separate, professional, social media account for this purpose. The employee must enable administration and parents to access the employee's professional page.
    c. The employee shall not communicate with any student between the hours of 10:00 p.m. and 6:00 a.m. unless the employee has instructional responsibilities, including grading, making comments on digital student work and supervisory or safety concerns for the student at that time. An employee may, however, make public posts to a social network site, blog, or similar application at any time.
    d. Upon request from administration, an employee will provide the phone number(s), social network site(s), or other information regarding the method(s) of electronic media the employee uses to communicate with any one or more currently enrolled students through the employee's professional page or site.

e. Upon written request from a parent, the employee shall discontinue communicating with the parent's minor student through email, text messaging, instant messaging, or any other form of one-to-one communication.
f. An employee may request an exception from one or more of the limitations above by submitting a written request to his/her immediate supervisor. Any exception granted will be documented in writing by the immediate supervisor.

6. **Employee Personal Web Pages**
Employees may not misrepresent the District by creating, or posting any content to, any personal or non-authorized website that purports to be an official/authorized website of the District. No employee may purport to speak on behalf of the District through any personal or other non-authorized website.

7. **Retention of Electronic Communications and other Electronic Media**

a. 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.

8. **Compliance with Federal, State and Local Law**
a. For all electronic media, employees are subject to certain state and federal laws, local policies, and administrative regulations, even when communicating regarding personal and private matters, regardless of whether the employee is using private or public equipment, on or off District property. These restrictions include:
    i. Confidentiality of student records
    ii. Confidentiality of other District records, including educator evaluations and private email addresses.
    iii. Confidentiality of health or personnel information concerning colleagues, unless disclosure serves lawful professional purposes or is required by law.
    iv. Prohibition against harming others by knowingly making false statements about a colleague, student or the District.
    v. Prohibitions against soliciting or engaging in sexual conduct or a romantic relationship with a student.

9. **Disclaimer**

The District's electronic 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 electronic communications system.

LEGAL REF.: Sections 19.31 to 19.37 Wisconsin Statutes
19.62 to 19.80
118.125
120.12(1)
943.70
947.0125
995.55(3)

Chapter 19, Subchapters II and IV
ADM 12, Wisconsin Administrative Code
Children's Internet Protection Act
Protecting Children in the 21st Century Act Amendment
Children's Online Privacy Act
Federal Copyright Law [17 U.S.C.]
Technology Education and Copyright Harmonization Act (TEACH Act)
E-rate funding requirements
Electronic Communications Privacy Act [18 U.S.C. § 2510-2522)
Federal Family Educational Rights and Privacy Act

CROSS REF.: 347, Student Records
363.1 District's Safe and Acceptable Use of Internet and Electronic Resources/Media for Students
411.1 Bullying of Students and Staff
511, Equal Opportunity Employment
512, Harassment
771.1, Use and Duplication of Copyrighted Materials
823, Access to Public Records
Current Employee Agreements

Approved: August 2002

Revised: March 2005
July 2, 2013
September 11, 2014