MIDDLETON-CROSS PLAINS AREA SCHOOL DISTRICT

Administrative Policy and Procedure Manual

363.1

DISTRICT'S SAFE AND ACCEPTABLE USE OF INTERNET AND ELECTRONIC RESOURCES/MEDIA FOR STUDENTS

Policy

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

Procedure for Acceptable Use

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, 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 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 to the following list: 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 and electronic resources is a privilege which may be revoked at any time for cause. 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, expulsion, exclusion; or civil or criminal liability under other applicable laws.

2. **User Responsibilities**
Students are responsible for their actions in accessing available electronic resources. In addition to the tenets of the Academic Integrity Policy, the following standards will apply to all students:

    a. The student in whose name a system account is issued will be responsible at all times for its proper use. Students may not access another user's account or intentionally delete or damage the property or data of another user.
    b. Students shall not engage in any activity that disrupts or hinders the performance of the District's electronic technologies.
    c. Each student is responsible for his or her password security and may not share his or her password with another student under any circumstances.
    d. Students will not use the District's electronic technologies for political campaigning, personal businesses or profit generating purposes.
    e. The system may not be used for illegal purposes, in support of illegal activities, or for any other activity prohibited by District policy.
    f. Students shall not impersonate another user on either the District network or the public networks. State statutes may be utilized to refer individuals to law enforcement as appropriate.
    g. A student 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.
    h. A student may not disable Internet tracking software or implement a private browsing feature on District computers or networks. Browsing history shall only be deleted by authorized staff or in accordance with the District's technology department's directives.
    i. Students 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, including that of the individual student.
        e. Any content that constitutes privacy invasion, harassment or bullying as defined by Administrative Policy 411 or 443.4.

3. **Personal End User Devices**

    a. Personal end-user devices (e.g. laptops, tablets, smart phones, etc.) are not managed or supported by the district. Students are solely responsible for any personal device that they bring on District property.
    b. Students shall only use personal devices that they own or have the express permission from the owner to use.

c. Personal devices may only be connected to the District's wireless access and never physically plugged into a network drop.
d. Users of personal devices, when on district property or engaged in school related activities, are expected to adhere to the standards in Section 2, regardless of the network they are connected to, including non-district networks.
e. Students may use personal devices in academic settings (classrooms, library, resources) at the discretion of MCPASD Staff.
f. By exercising the privilege of bringing a cell phone or other electronic devices to school or school-sponsored events, the student and parents knowingly and voluntarily consent to the search of the device when school officials have a reasonable suspicion that such a search will reveal a violation of school rules. The scope of the search will be limited to the violation of which the student is accused. School officials as part of the search may request or require the student to disclose access information to enable access or observation of the contents of the electronic device, but school officials shall not request or require a student to disclose access information for the personal internet account(s) of the student.

4. **Parents' Responsibility – Notification of Student Internet Use**
Outside of school, parents bear responsibility for the same guidance of Internet use as they exercise with information sources such as television, telephones, radio, movies and other possibly offensive media. Parents are responsible for monitoring their student's use of the District's educational technologies and of the Internet if the student is accessing the District's electronic technologies from home or through other remote location(s).

Parents will be notified that their students will be using District resources/accounts to access the Internet and will be provided a copy of the District's Acceptable Use for Internet and Electronic Media for their review.

Safe Use of the Internet and other Electronic Resources/Media

Consistent with applicable federal laws, the District believes that the best approach to student safety as it relates to use of the Internet and other electronic resources involves a combination of technology protection measures, monitoring and instruction. The District's comprehensive approach to student Internet/technology safety shall take into account the differing ages and instructional levels of the students in the District.

It shall be the responsibility of the Director of Technology to:

1. Ensure that the District's systems and equipment that provide access to the Internet make active use of technology protection measures designed to block or filter Internet access to visual depictions that are:

   a. obscene;

   b. pornographic; or

   c. as to computers and other devices that may be accessed by students or other minors, otherwise harmful to minors.

Filtering, blocking or other protective technologies will also be used to decrease the likelihood that student users of the District systems and equipment might access other materials or communications, other than visual depictions, that are inappropriate for students. Recognizing that there will always be room for possible improvement in connection with the District's efforts at prevention, all employees, parents and guardians, and students are encouraged to report to the Director of Technology or building principal any complaints or concerns regarding student access or exposure to any content, activities or communications that may be harmful, deceptive, or otherwise inappropriate or objectionable.

2. Develop and implement procedures that provide for the monitoring of students' and other authorized users' activities when using District-provided equipment or District-provided network access or Internet access. Such monitoring may sometimes take the form of direct supervision of students' and minors' online activity by school personnel, but the District recognizes that constant, direct supervision is not a practical expectation.

3. Develop and implement an instructional program that is designed to educate students about acceptable and responsible use of technology and safe and appropriate online behavior, including (a) safety and security issues that arise in connection with various forms of electronic communication (such as e-mail, instant messaging, and similar technologies); (b) interacting with other individuals on social networking sites and in chat rooms; and (c) cyber bullying awareness and response. Such educational activities shall include (but shall not consist exclusively of) reinforcement of the provisions of the District's rules regarding students' acceptable and responsible use of technology while at school.

4. Maintain, revise and enforce rules and procedures concerning the acceptable, safe, and responsible use of the District's Internet access infrastructure and other technology-related District resources by any person who is authorized to use the District's systems and equipment, including any student, District employee, District official, or other authorized user that is consistent with the policy provisions set forth above. These rules and procedures shall complement structural and systemic supports that are implemented to further encourage and facilitate the acceptable, safe, and responsible use of the District's technology-related resources. To the extent appropriate to various groups of users, and with all such additions as the administration deems necessary or appropriate, those rules and procedures shall:

    a. Address and prohibit the unauthorized collection, disclosure, use and dissemination of personal and personally-identifiable information regarding students and minors, as particularly applicable to technology-based resources;

    b. Address employees' obligations regarding the proper retention of District records, maintaining the confidentiality of student records, and avoiding inappropriate disclosures of District records;

    c. Prohibit unauthorized user access to systems, networks and data;

    d. Prohibit the use of District resources to access and/or transmit inappropriate material via the Internet, electronic mail, or other forms of electronic communications;

e. Provide notice to users that there is no District-created expectation of privacy in their use of District technology resources. Accordingly, except where prohibited by state or federal law: (1) the District reserves the ability to track, monitor, and access all data, files, communications, or other material that users create, store, send, delete, receive, or display on or over the District's Internet connection, network resources, file servers, computers or other equipment; and (2) all aspects of any individual's use of the District's technology-related equipment and resources, including any online activities that make use of District-provided Internet access, may be monitored and tracked by District officials. The District may through such review of all data, files, communications, or other material that users create, store, send, delete, receive, or display on or over the District's internet connection, network resources, file servers, computers or other equipment inadvertently obtain access information for an employee's or student's personal internet account. 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.; and

f. Provide notice to users regarding possible consequences for violations of the policies, rules and procedures that govern the acceptable, safe, and responsible use of the District's technology-related resources.

Building principals or his/her designee shall have responsibility, within their respective schools, for overseeing the day-to-day implementation of the District's policies, rules and guidelines regarding the acceptable, safe, and responsible use of technology resources. A building principal or his/her designee, in consultation with the Director of Technology as needed, may approve modified levels of Internet filtering/blocking for an individual user account provided that there is a legitimate educational purpose and any changes in access will not compromise the overall adequacy of protections that are in place for student users.

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 120.12(1) Wisconsin Statutes
120.12(2)
120.13(1)(a)
120.18(1)(i)
943.70
947.0125
995.55(3)
PI 8.01(2)(k)

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

CROSS REF.: 310, Philosophy of Educational Programs, Instruction and Materials
330, Curriculum Development and Improvement
333, Parent Rights and Access to the Curriculum and Instructional Materials
343.6, Videotaping and/or Photographing of Students
347, Student Records
361, Selection, Review and Disposal of Instructional Materials and Textbooks
411, Equal Educational Opportunities
411.1 Bullying of Students and Staff
443, Student Conduct and Discipline
455.1, Supervision of Students
522.7, Staff Internet Acceptable Use
771.1, Use and Duplication of Copyrighted Materials

APPROVED: August 2002

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