ADMINISTRATIVE POLICIES OF THE MILWAUKEE PUBLIC SCHOOLS

ADMINISTRATIVE POLICY 6.34
STAFF INTERNET SAFETY ACCEPTABLE USE POLICY (AUP)

Milwaukee Public Schools offers electronic network access for students, teachers, and other staff within the school system. The purpose of having the electronic network is to support the instructional program, including learning opportunities, business applications, information retrieval, searching strategies, research skills, and critical thinking. This document defines the acceptable use of the MPS network system (i.e., WAN, LAN, Internet, digital platforms, and email) and computer resources by MPS Staff, as well as the obligation of school staff to educate, supervise, and monitor appropriate usage by students.

(1) EDUCATIONAL PURPOSE

(a) The district's network system has been established for educational and administrative purposes. The term *educational purpose* includes classroom activities, continuing education, professional or career development, and high-quality, educationally enriching personal research.

(b) The district's network system has not been established as a public access service or a public forum. The district has the right to place restrictions on the material which staff accesses or posts through the system. Staff is also expected to follow the rules set forth in this policy and the law in staff's use of the network system. Disciplinary action may take place against MPS staff that breaks rules, as defined in MPS administrative policy.

(c) Staff may not use the network system for commercial purposes. This means that staff may not offer, provide, or purchase products or services through the network system.

(2) RULES AND REGULATIONS

(a) Acceptable Use

Milwaukee Public Schools' networks are to be used in a responsible, efficient, ethical, and legal manner and must be in support of the educational objectives and employee guidelines of Milwaukee Public Schools.

(b) Unacceptable Use

1. Unacceptable use includes, but is not limited to, the following:
    a. violation of copyright/trademark laws;
    b. use of threatening or obscene material;
    c. political or campaign materials;
    d. sending or soliciting sexually-oriented messages or images;
    e. changing settings on computers;
    f. disrupting the network through casual use of the Internet;
    g. accessing chat services and other social media sites, except those set up and/or approved by school administration;
    h. accessing programs not appropriate for educational use;
    i. unauthorized use of district applications ;
    j. access to pornography, including child pornography.
2. The use of the email system is permitted as long as it is used for educational purposes.3. Listservs may never be used for personal emails, nor may the employee use district-wide school or department email addresses.

4. Use of offensive or harassing statements or language, including profanity, vulgarity, and/or disparagement of others based on their race, national origin, sex, sexual orientation, age, disability, or religious or political beliefs, is prohibited.

5. Staff shall not cyberbully another person. Cyberbullying includes, but is not limited to, the following misuses of technology: harassing, teasing, intimidating, threatening, or terrorizing another staff member or student by way of any technological tool, such as sending or posting inappropriate or derogatory email messages, instant messages, text messages, digital pictures or images, or social media website postings.

6. Staff shall not engage in the unauthorized disclosure, use, or dissemination of personal identifiable information (PII) regarding students. "Personal identifiable information" includes the student's full name, together with other information that would allow an individual to locate the student, including the student's family names, the student's home address or location, the student's work address or location, or the student's phone number.

(3) EDUCATION, SUPERVISION AND MONITORING

(a) It shall be the responsibility of the Chief Academic Officer and Director of Technology to educate, supervise, and monitor usage of the online computer network and access to the Internet in accordance with this policy, the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act, and the Protection Children in the 21st Century Act.

(b) Procedures for the disabling or otherwise modifying of any technology-protection measures shall be the responsibility of the Director of Technology or designated representatives.

(c) The Chief Academic Officer or designated representatives shall provide appropriate training for staff who use the MPS network system . The training provided will be designed to promote the district's commitment to:

1. the standards and acceptable use of Internet services as set forth in the MPS Acceptable Use Policy;
2. staff and student safety with regard to:
    a. safety on the Internet;
    b. appropriate behavior while on online, on social media Web sites, and in chat services ; and
    c. cyberbullying awareness and response; and
3. compliance with the E-rate requirements of the Children's Internet Protection Act ("CIPA").

Following receipt of this training, participating staff will acknowledge that they have received the training, and will follow the MPS Safety Acceptable Use Policy (AUP).

(d) CIPA definition of terms:

1. **Minor.** The term *minor* means any individual who has not attained the age of 17 years.
1. **Technology-Protection Measure.** The term *technology-protection measure* means a specific technology that blocks or filters Internet access in visual depictions that are:
    a. *obscene,* as that term is defined in section 1460 of Title 18, United States Code;
    b. *child pornography,* as that term is defined in section 2256, of Title 18, United States Code; or
    c. harmful to minors.
2. **Harmful to Minors.** The term *harmful to minors* means any picture, image, graphic image file, or other visual depiction that:
    1. taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;

2. 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; and
3. taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

(4) SYSTEM SECURITY AND RESOURCE LIMITS

(a) System Security

1. Attempts to login to the system as any other user, to share a password, or to allow a security breach may result in cancellation of user privileges.

2. Staff will immediately notify the MPS Technology Department if they have identified a possible security problem. Staff, however, shall not look for security problems, because this may be construed as an unlawful attempt to gain access. Staff shall not demonstrate any such problem to other users. Communications relating to, or in support of, illegal activities may be reported to the authorities.

3. Staff will avoid the inadvertent spread of computer viruses by following the district's virus-protection procedures.

(b) Resource Limits

Staff will not download files unless absolutely necessary for educational or administrative purposes. If deemed necessary, staff shall immediately remove the file from the computer/network after there is no longer a need to access it. Any files found to be non-educational or unrelated to the business of the district may be removed without notice.

(5) EMAIL ACCOUNTS

(a) Email accounts are to be used only by their owners.

(b) Electronic mail is not guaranteed to be private: system operators have access to all mail.

(c) All staff email is archived in accordance with the Open Records Act.

(6) PRIVACY

(a) Privacy

1. Staff should expect only limited privacy in the contents of their personal files on the network system and records of their online activity. This district's monitoring of Internet usage can reveal all activities in which staff engage in using the MPS network system.

2. Routine maintenance and monitoring of the MPS network system may lead to discovery that staff has violated this policy or the law. An individual search will be conducted if there is reasonable suspicion that staff has violated this policy or the law. The investigation will be reasonable and related to the suspected violation.

3. Confidential files are to be accessed only by appropriate personnel.

(b) Due Process

1. The district will cooperate fully with local, state, or federal officials in any investigation related to any unlawful activities conducted through the MPS network system.

2. In the event there is a claim that a member of the staff has violated this policy in their use of the network system, he/she will be provided with notice and opportunity to be heard in the manner set forth in administrative policy.

(7) LIMITATION OF LIABILITY

The district will not guarantee that the functions or services provided through the network system will be without error. The district will not be responsible for any damage which staff may suffer, including,

but not limited to, loss of data, interruptions of service, or exposure to inappropriate material or people. The district will not be responsible for the accuracy or quality of the information obtained through the MPS network system. The district will not be responsible for financial obligations arising through the unauthorized use of the system.

History: Adopted 1-25-2007; Revised 6-24-10; 6-28-12; 6-27-24

Cross Ref.:

Admin. Policy	8.47	Children's Internet Protection Act
Admin. Policy	8.48	Student Internet Safety Acceptable Use Policy (AUP)

— ◊ —