ADMINISTRATIVE POLICY 8.48 STUDENT INTERNET SAFETY AND ACCEPTABLE USE POLICY (AUP)

This document defines for students the acceptable use of the MPS network system (i.e., WAN, LAN, Internet, email, ~~computer,~~ and digital platforms ~~other technological resources~~). Following this policy allows students to use the Internet in a safe and responsible manner.

(1) PURPOSE

(a) The district's network system has been established for educational and administrative purposes. The term *educational purposes* 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 students access or post through the system. Students are also expected to follow the rules set forth in this policy, the student disciplinary code, and the law in their use of the district's network system. Teachers, counselors, administrators, and other school personnel may take disciplinary action against MPS students who break rules. Disciplinary actions are set according to federal and state laws and MPS administrative policies.

(c) Students may not use the district's network system for commercial purposes. This means students may not offer, provide, or purchase products or services through the district's network system.

(2) ACCESS TO ONLINE MATERIALS

(a) The material which students access through the district's network system should be for class assignments or for personal research on subjects similar to those that a student might study in a class or in the school library. Use for entertainment purposes is not allowed.

(b) Students shall not use the district's network system to access the following:

1. material that is obscene;
2. pornography, including child pornography;
3. material that depicts, or describes in an offensive way, violence, nudity, sex, death, or bodily functions;
4. material that has been designated as for adults only;
5. material that promotes or advocates illegal activities;
6. material that promotes the use of alcohol or tobacco or school cheating, or material that advocates participation in hate groups or other potentially dangerous groups;
7. material that is deemed harmful to minors.

(c) If a student mistakenly accesses inappropriate information, ~~he/she~~ they should immediately report this access in the manner specified by ~~his/her~~ their school. This will protect the student against any claim that ~~he/she has~~ they have intentionally violated this policy.

(d) The district has installed technology-protection measures to block access to inappropriate material and to visual depictions deemed obscene, child pornography, or harmful to minors.

1. If a student feels that the filtering software is blocking access to an appropriate site, the student should report this to the school's library media specialist, instructional technology leader, principal, or teacher.
2. Students shall not seek to bypass the filtering software by using a proxy site or some other technology.

(e) New technologies are being invented constantly, and it is impossible to predict what systems or applications will be available for use in the future. This policy applies to all technologies currently in use on the MPS network, as well as those technologies that may be used on the MPS network in the future.

(3) EDUCATION, SUPERVISION AND MONITORING

(a) It shall be the responsibility of all members of the school staff to educate, to supervise, and to monitor appropriate 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 will provide age-appropriate training for students who use the school's Internet ~~facilities~~. The training provided will be designed to promote the school's commitment to:

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

~~Following receipt of this training, the student will acknowledge that he/she they received the training, understood it, and~~ The student will follow the provisions of the MPS Internet Safety and Acceptable Use policies.

(d) CIPA definition of terms:

1. **Minor.** The term *minor* means any individual who has not attained the age of 17 years.
2. **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.
3. **Harmful to Minors.** The term *harmful to minors* means any picture, image, graphic image file, or other visual depiction that:
   a. taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
   b. 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
   c. 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. Students are responsible for their individual accounts and should take all reasonable precautions to prevent others from being able to use their accounts. Students should change their passwords ~~regularly~~ as required. Under no conditions should students provide their passwords to other people. Students should always log off the computer when they are finished.

2. The students shall immediately notify a teacher or another school employee if the student has identified a possible security problem. Students, however, shall not look for security problems, as this may be construed as an unlawful attempt to gain access.

3. Students shall avoid the inadvertent spread of computer viruses by following the district's virus-protection procedures. Students shall request permission to download applications and shall avoid downloading suspicious software from unprotected sites. Students shall immediately notify the Information Technology Department (Support) if they have identified a possible security problem. However, Students shall not go looking for security problems, because this may be construed as an illegal attempt to gain access.

(b) Resource Limits

1. Students shall use the system only for educational and career-development activities and limited, high-quality personal research.

2. Students shall download only those files (e.g., music files and images) deemed necessary for educational purposes, with the instructor's permission. The files shall be removed from the network after students no longer need access to them. Any files found to be non-educational in nature may be removed without notice.

(5) COMMUNICATION SAFETY

Students shall not disclose names, personal ~~contact~~ identifiable information (PII), or any other private or personal information about themselves or other students or, or staff, or other adults. ~~minors.~~ This includes not entering personal identifiable information into Artificial Intelligence tools. "Personal ~~contact~~ 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 name, the student's home address or location, the student's work address or location, or the student's phone number.

(6) UNLAWFUL, UNAUTHORIZED AND INAPPROPRIATE USES

(a) Unlawful Activities

1. Students shall not attempt to gain unauthorized access to the district's network system or to any other computer system through the district's network system, nor shall they go beyond their authorized access. This includes attempting to log in through another person's account or to access another person's files.

2. Students shall not make deliberate attempts to disrupt the district's network system or any other computer system or to destroy data by spreading computer viruses or by any other means.

3. Students shall not use the district's network system to engage in any other unlawful act, including, but not limited to, arranging for a drug sale or the purchase of alcohol or weapons, engaging in criminal gang activity, or threatening the safety of any person.

(b) Inappropriate Language and images

1. Restrictions against inappropriate language apply to all speech communicated through the district's network system, including public messages, private messages, and material posted on the Internet ~~Web pages, wikis and blogs,~~ or any other social ~~networking~~ media sites.

2. Students shall not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language.

3. Students shall not post information that could cause damage or a danger of disruption to their schools or to any other organizations or persons.

4. Students shall not engage in personal attacks, including prejudicial or discriminatory attacks.

5. Students shall not harass or bully other persons. Students shall not ~~cyber-bully~~ cyberbully other persons. ~~Cyber-bullying~~ Cyberbullying includes, but is not limited to, the following misuses of technology: harassing, teasing, intimidating, threatening, or terrorizing another student or staff member

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. Students shall not knowingly or recklessly post false or offensive information about a person or organization.

7. ~~A students~~ Students shall promptly disclose to ~~his/her~~ their teachers or other school employees any messages that the student receives from any other person that is in violation of the restrictions on inappropriate language.

(c) Plagiarism and Copyright Infringement

1. Students shall not plagiarize work that they find on the Internet. Plagiarism is taking the ideas or writings of others, including the use of Artificial Intelligence in any capacity, and presenting them as if they were one's own.

2. Students shall respect the rights of copyright owners in their use of materials found on, disseminated through, or posted to the Internet. Copyright infringement occurs when one inappropriately reproduces a work that is protected by a copyright.

(7) PRIVACY

1. Students should expect only limited privacy in the contents of their personal files on the district's network system and records of their online activity.

2. The district will cooperate fully with local, state, and federal officials in any investigation related to any unlawful activities conducted through the district's network system and/or district issued device.

(8) VIOLATIONS OF THIS ACCEPTABLE USE POLICY

Violations of this policy may result in loss of access as well as other disciplinary and/or legal action in accordance with administrative policy. A student's violation of this policy shall be subject to the consequences as indicated within this policy, as well as other appropriate discipline. Disciplinary actions will be tailored to meet specific concerns related to the violation. ~~and to assist the student in gaining the self-discipline necessary to behave appropriately on an electronic network.~~ If the violation also involves a violation of other provisions of other school rules, it will be handled in a manner described in the school rules. Additional restrictions may be placed on a student's use of ~~his/her~~ their network account.

(9) LIMITATION OF LIABILITY

The district will not guarantee that the functions or services provided through the district's network service will be without error. The district will not be responsible for any damage which the student 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 system. The district will not be responsible for financial obligations arising through the unauthorized use of the system. A student's parents may be held financially responsible for any harm that may result from the student's intentional misuse of the system.

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

Cross Ref.:

Admin. Policy	8.47	Children's Internet Protection Act
Admin. Policy	6.34	Staff Internet Safety Acceptable Use Policy (AUP)

— ◊ —