Student Technology Acceptable Use Policy
IM 4.160

METROPOLITAN Nashville PUBLIC SCHOOLS

Date Published
July 2010

Revision History
January 2010

Review
Annually

Metropolitan Nashville Public Schools recognizes that the effective use of electronic media and telecommunications networks enhance the quality and delivery of education in our schools by providing access to unique resources and opportunities for collaborative work.

However, the use of electronic technology is a privilege and is subject to all applicable state and federal laws and policies of the district. MNPS reserves the right to examine electronic mail messages, files on all types of MNPS computers and servers, web browsers, cache files, websites, website logs and any other information stored or passing through our information systems. Parents will be required to sign an Acceptable Use Agreement, which will be kept on file at each school, for student who wishes to access the MNPS network.

At no time shall there be an expectation of privacy by students while utilizing any MNPS network, stand-alone system, or other device. The district reserves the right to examine any information originating on, accessed by or processed through MNPS owned computers, networks or other information system components. This examination may occur with or without the user's prior knowledge and may be conducted in real time or by examining access history and/or related files. Users should be aware that electronic communications could, depending on the technology, be forwarded, intercepted, printed and/or stored by others. Electronic communications are also retrievable after the user has deleted them from his/her system, so it is best practice not to store personal confidential information on a district machine or server.

In accordance with federal law, MNPS shall ensure the safety of students through strict enforcement of acceptable use guidelines and a filtered network that is consistently monitored for unacceptable content pursuant to 47 USC §254(h) and the Children's Internet Protection Act (CIPA).

Alleged violations involving student use shall be reported to the teacher who was supervising the student at the time of the alleged offense. The teacher or staff person shall report the alleged violation to the principal, who will investigate the incident, with appropriate input from the Information Technology department. If after the investigation there is a reasonable certainty that a violation actually occurred, the principal will impose sanctions, which may include limiting or suspending a student's internet privileges. Serious or repeated violations of internet or e-mail use could result in permanent loss of internet and/or e-mail privileges, and other disciplinary action consistent with the Student Code of

Conduct. If a student's misuse of internet or e-mail is in violation of the law, such misuse shall be reported to the appropriate authorities and could be punished as a criminal offense.

Metro Nashville Public Schools
STUDENT GUIDELINES FOR ACCEPTABLE USE OF MOBILE COMPUTING DEVICE

These guidelines are provided so that students and parents are aware of the responsibilities students accept when they use District-owned computer hardware, operating system software, application software, stored text, data files, electronic mail, local databases, CDROMs, digitized information, communication technologies, and Internet access. In general, this requires efficient, ethical, and legal utilization of all technology resources.

Expectations for Use

1. Student use of computers, other technology hardware, software, and computer networks, including the Internet, is only allowed when supervised or granted permission by a staff member.

2. All users are expected to follow existing copyright laws. Copyright guidelines are posted and/or available in the media center of each campus as well as posted on the District's Web site.

3. Although the District has an Internet safety plan in place, students are expected to notify a staff member whenever they come across information or messages that are inappropriate, dangerous, threatening, or make them feel uncomfortable.

4. Students who identify or know about a security problem are expected to convey the details to their teacher without discussing it with other students.

Unacceptable Use

1. Using the network for illegal activities includes violating copyright laws, downloading software without the proper license, or contract violations or downloading inappropriate materials, installing viruses and/or similar software, such as but not limited to hacking and host file-sharing software.

2. Using the network for financial or commercial gain, advertising, or political lobbying.

3. Accessing or exploring online locations or materials that do not support the curriculum and/or are inappropriate for school assignments, such as but not limited to pornographic sites.

4. Vandalizing and/or tampering with equipment, programs, files, software, system performance, or other components of the network. Use or possession of hacking software is strictly prohibited.

5. Causing congestion on the network or interfering with the work of others, e.g., chain letters or broadcast messages to lists or individuals.

6. Intentionally wasting finite resources, i.e., online time, real-time music.

7. Gaining unauthorized access anywhere on the network.

8. Revealing the home address or phone number of one's self or another person.

9. Invading the privacy of other individuals.

10. Using another user's account, password, or ID card or allowing another user to access student's personal account, password, or ID.

11. Coaching, helping, observing, or joining any unauthorized activity on the network.

12. Posting anonymous messages or unlawful information on the system.

13. Engaging in sexual harassment or using objectionable language in public or private messages, e.g., racist, terroristic, abusive, sexually explicit, threatening, demeaning, stalking, or slanderous.

14. Falsifying permission, authorization, or identification documents.

15. Obtaining copies of or modifying files, data, or passwords belonging to other users on the network.

16. Knowingly placing a computer virus on a computer or network.

Acceptable Use Guidelines for the District's Network Computer Online Services

1. General Guidelines:
   a. Students will have access to all available forms of electronic media and communication that is in support of education and research, and in support of the educational goals and objectives of the District.

   b. Students are responsible for their ethical and educational use of the computer online services in the District.

   c. All policies and restrictions of the District's computer online services must be followed.

   d. Access to the District's computer online services is a privilege and not a right. Each employee, student, and/or parent will be required to sign the Acceptable Use Policy Agreement Sheet and adhere to the Acceptable Use Guidelines in order to be granted access to District computer online services.

   e. The use of any District computer online services in the District must be in support of education and research and in support of the educational goals and objectives of the District.

   f. When placing, removing, or restricting access to specific databases or other District computer online services, school officials will apply the same criteria of educational suitability used for other education resources.

g. Transmission of any material that is in violation of any federal or state law is prohibited. This includes, but is not limited to confidential information, copyrighted material, threatening or obscene material, and computer viruses.

h. Electronic mail, network usage, and all stored files will not be considered confidential and may be monitored at any time by designated District staff to ensure appropriate use.

i. Any attempt to alter data, the configuration of a computer, or the files of another user without the consent of the individual, campus administrator, or technology administrator, will be considered an act of vandalism and subject to disciplinary action in accordance with the District's Student Code of Acceptable Behavior.

j. Any parent wishing to restrict their children's access to any District computer online services will provide this restriction request in writing to the school administrator. Parents will assume responsibility for imposing restrictions only on their own children.

2. Network Etiquette:
   a. Be polite.

   b. Use appropriate language and appropriate keying etiquette (Example: using all caps is considered yelling).

   c. Do not reveal personal data (picture of yourself, home address, phone number, phone number of other people, picture of others).

   d. Remember that the other users of the District's computer online services and other networks are human beings whose culture, language, and humor have different points of reference from your own.

   e. Users should be polite when forwarding e-mail. The intent of forwarding email should be on a need-to-know basis.

3. E-Mail:
   a. E-mail should be used for educational or administrative purposes only.

   b. E-mail transmissions, stored data, transmitted data, or any other use of the District's computer online services by students, employees, or any other user shall not be considered confidential and may be monitored at any time by designated staff to ensure appropriate use.

   c. All e-mail and all e-mail contents are property of the District.

Consequences for Misuse

1. The student in whose name a system account and/or computer hardware is issued will be responsible at all times for its appropriate use.

2. Noncompliance with the guidelines published here and in the Student Code of Acceptable Behavior may result in suspension or termination of technology privileges and disciplinary actions. Use or possession of hacking software is strictly prohibited and violators will be subject to consequences of the Student Code. Violations of applicable state and federal law, including the Tennessee Code, Computer Crimes, Chapter 39 will result in criminal prosecution, as well as disciplinary actions by the District.

3. The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to violations of computer crime laws. Contents of e-mail and network communications are governed by the Tennessee Open Records Act; therefore, proper authorities will be given access to their content.

References/Authority

Children’s Internet Protection Act (CIPA) 47 USC §254(h)(1)
Family Educational Rights and Privacy Act (FERPA) 20 USCA §1232(G)
TCA §10-7-512
TCA §39-14-602
TCA §39-14-105
17 USCA §107, 117
MNPS Student Code of Conduct
Student Technology Acceptable Use Form (MNPS Form Available on policy.mnps.org)
Appendix A- MNPS ACCEPTABLE USE AGREEMENT Form

MNPS ACCEPTABLE USE AGREEMENT (Appendix A)

PLEASE PRINT
ALL INFORMATION

Student Section

Please **block print** the students name, one letter in each block.

First name																		
Middle name																		
Family name																		

I have read the Student Technology Acceptable Use Policy IM 4.160. I understand that the following actions are prohibited: copyright infringement, electronic theft, the creation of or consumption of pornography or gratuitous violence, harassment, abuse,stalking, invasion of privacy, slander, use for commercial or political purposes, interference with others in the process of their work, or any other illegal, or unethical activities. I agree to follow the rules contained in the policy. If I violate the rules I will lose my access privilege to the District's computer online services and may face disciplinary action. I will not: leave devices in lockers overnight or unlocked, carry them in heavily loaded book bags or back packs, leave them in unattended vehicles, or unsecured rooms, loan them to others or cause them to be unsecured or in a precarious situation either by action or failure to act.

Student signature

Date

Attach Asset Tag Number Here:

Parent section

I have read the Student Technology Acceptable Use Policy. I understand that the Internet is a worldwide group of hundreds of thousands of computer networks. I agree that MNPS does not control the content of these Internet networks. I understand that if my child violates the Acceptable Use Guidelines, his/her access privilege to the District's computer online services may be revoked and may be subject to disciplinary action.

Metro Nashville Public Schools has my permission to give network and Internet access to my child. I understand that my child will maintain this privilege as long as procedures described in the District's Acceptable Use Guidelines are followed.

Parent or Guardian signature

Date

Parent name (print)

Home address

Phone

INVENTORY SHEET
(Only applicable if provided a district-owned device)

Check-out **Student Name:**
Student ID#: **Asset Tag #:**

Date: ______________ **Time:** __________________

Inventory	IT Rep. Initials	Student Initials
Battery present/charged		
System powers on		
Laptop bag, power supply cords, and network cable		
CD/DVD drive present		

Notes/cosmetic damage:

Checked out by: ____

AP/Honors/ Classroom Teacher/Librarian Name (please print)

Check-out **Student Name:**
Student ID#: **Asset Tag #:**

Date: ______________ **Time:** __________________

Inventory	IT Rep. Initials	Student Initials
Battery present/charged		
System powers on		
Laptop bag, power supply cords, and network cable		
CD/DVD drive present		

Notes/cosmetic damage:

Checked in by:

____

IT Rep. Name (please print)