Technology Acceptable Use Policy
HC 5.112
IM 4.160

METROPOLITAN Nashville PUBLIC SCHOOLS

Revision History
January 2014
August 2012
May 2012
July 2010
January 2010

Review
Annually

Date Last Reviewed
January 2014

Metropolitan Nashville Public Schools recognizes that the effective use of technology enhances the quality of education in our schools by enabling access to unique sources of information and by providing significant opportunities for collaborative work.

1. Purpose. This policy will establish standards for the acceptable use of technology by students, staff members, and visitors to MNPS facilities. Attachments to this policy will provide mechanisms for implementing various sections of this policy

2. Definitions.

   a. "Student". For the purposes of this policy a "Student" is defined as any individual enrolled in a class at any MNPS school or MNPS supervised charter school.

   b. "Staff Member". For the purposes of this policy a "Staff Member" is defined as any employee of MNPS, any contractor employed by a company that is providing paid services to MNPS, or any employee or contractor of a charter school under the supervision of MNPS

   c. "Visitor". For the purposes of this policy a "Visitor" will be defined as any non-employee of MNPS that is accessing any technology resource within any facility that is owned by MNPS or occupied and used by MNPS staff members.

   d. "Parent". For the purposes of this policy, a "Parent" will be defined as a natural or adoptive parent or other person acting in the capacity of a parent (step-parent, grandparent, guardian, etc.)

   e. "Users". For the purposes of this policy, a User will be defines as a collective group that is comprised of Students, Staff Members and Visitors.

   f. "Technology Resource". For the purposes of this policy, a "Technology Resource" will be defined as any Local Area network; Wide Area Network or any

telecommunications circuit whether wired or wireless, that is used to access the Internet or any information source that is, or is not owned or controlled by MNPS; or any computing device, regardless of operating system or form factor.

g. "Account". For the purposes of this policy, an "Account" will be defined as any Active Directory account or other set of credentials consisting of a unique username and password that are collectively designed to authenticate the user's identity for the purpose of providing access to MNPS technology resources.

3. General Policies. The use of technology resources by students, staff members, or visitors to MNPS is a privilege and is subject to all applicable state and federal laws and policies of the district. Students are responsible for their ethical and educational use of the computer online services in the District.

   a. Account Usage. The user for whom an account is created is assumed to be responsible for all activities that occur in connection with the use of this account.

   b. Expectation of Privacy. All MNPS technology resources, and all information process by, created on, or transmitted through MNPS technology resources are subject to the provisions of applicable Public Records laws. **At no time shall there be an expectation of privacy by students, staff, parents, visitors or contractors while utilizing any MNPS technology resource, any MNPS network, stand-alone system, or other device.** The district reserves the right to examine, at their sole discretion, 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.

   c. Monitoring and Reporting Alleged Policy Violations.

      1) System administrators will not routinely monitor user Internet, social media, online services and e-mail activities, except for student users in order to protect students from unacceptable content. MNPS will take reasonable precautions to protect user privacy. However, MNPS may monitor a user's Internet, online services and/or e-mail activity when there is a legitimate business or technical need to do so. Circumstances that would warrant this level of access or monitoring include, but are not limited to:

         a) When there is a need to access information when a user is absent for an extended period of time or unavailable to assist technical personnel
         b) When there is a need to diagnose and/or resolve technical problems involving system hardware, software or communications
         c) As an incidental activity when conducting network maintenance
         d) When there is a need to gather information required for litigation

e) As a part of testing performed by auditors
f) When a reasonable suspicion exists that a user is engaging in unprofessional and/or illegal activities that are facilitated by or otherwise involve use of the MNPS network
g) As a part of an investigation of a possible crime or violation of MNPS policy
h) When there is a legal requirement to disclose e-mail or internet activity to law enforcement officials
i) When there is a request for access to information under the Open Records Act

2) Alleged violations involving employees shall be reported to the appropriate principal or department head, which will investigate the incident with input from the Information Technology Department. Clear and willful violations or abuse of acceptable usage as set forth in this policy will be subject to disciplinary actions, depending on the severity of the transgression and policy abuse, up to and including termination. Criminal or civil action may be initiated if the violation involves action that is against the law.

d. Data Security. Users should be aware that electronic communications could, depending on the technology, be forwarded, intercepted, printed and/or stored by third parties, even if these communications occur on MNPS owned systems or on MNPS owned networks. Electronic communications are also retrievable after the user has deleted them from his/her system. It is best practice to not to store personal confidential information on a district resource.

e. Respect for Copyrighted information. 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. 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. Users may access copyrighted material for research purposes, but its use must strictly adhere to the agreement posted by the author and/or current copyright law (17 USC §101).

f. Network Filtering. MNPS will undertake good faith efforts to ensure that MNPS users are provided filtered Internet access that prevents access to unacceptable content. All users and parents should understand that despite good faith efforts at network filtering, objectionable content might be available either as a result of the users using unauthorized techniques designed to bypass filtering or as a result of the creation of objectionable content that has not yet been identified by filtering software. Twitter and YouTube are approved social media sites that bypass some of MNPS's network filtering.

g. Enforcement of External Laws and Policies.

1) 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).

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

3) 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.

h. Unacceptable Use. MNPS Users will not engage in unacceptable use of technology resources. Unacceptable use consists of activities described below.

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) Accessing or transmission of threatening, offensive or harassing information (text or images) which contains defamatory, abusive, obscene, pornographic, profane, sexually oriented, racially offensive, or otherwise biased, discriminatory or illegal materials shall be strictly prohibited.

3) Transmission of incendiary statements that potentially might incite violence or describe or promote the use of weapons or devices associated with terrorist activities shall be strictly prohibited.

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

5) Attempting to subvert network security, impair the functionality of the network, or to bypass restrictions set by network administrators is forbidden. This includes creation and use of proxy servers.

6) Use of "system" or "administrative" passwords is prohibited by unauthorized individuals.

7) Downloading "pirated" copies of copyrighted music, video recordings, or unapproved or illegal software onto the MNPS network is prohibited.

8) 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 or sites that are intended to engage in or encourage the cyber bullying of MNPS students or staff.

9) 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.

10) Causing congestion on the network or interfering with the work of others, e.g., chain letters, broadcast messages to lists or individuals or video streaming of non-instructional material on MNPS or personal equipment using MNPS resources.

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

12) Gaining unauthorized access anywhere on the network.

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

14) Invading the privacy of other individuals.

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

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

17) Posting anonymous messages or unlawful information on the system.

18) Engaging in sexual harassment or using objectionable language in public or private messages, e.g., racist, terroristic, abusive, sexually explicit, threatening, demeaning, stalking, slanderous, or encourage the cyber-bullying of MNPS students or staff

19) Falsifying permission, authorization, or identification documents.

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

21) Knowingly placing a computer virus on a computer or network.

i. Network and E-Mail Etiquette

1) Be polite.

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

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

4) 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.

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

6) The distribution of chain letters, spam, advertisements and unauthorized solicitations is unacceptable and forbidden.

7) E-mail should be used for educational or administrative purposes only.

8) 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.

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

10) E-mail Signatures should look professional and represent the District and the views of the District, not personal viewpoints. The following items are permitted in the e-mail signature:
    - MNPS or School Logos
    - Employee's Name
    - Job Title
    - Address
    - Phone Numbers
    - E-mail Address
    - Office and/or Classroom Location
    - School Address and/or Contact Information
    - MNPS or School Icons and/or links for the District or School (homepage, portal, Twitter, Facebook, etc.)
    - MNPS Mission Statement
    - Confidentiality Statement

    Signatures may include all of the items above or any portion. No other items including pictures and quotations are permitted in the signature.

j. Disclaimer of Liability

1) MNPS makes no warranties of any kind, either express or implied, that the functions or the services provided by, or through, the MNPS network will be error-free or without defect. MNPS will not be responsible for any damage users may suffer, including but not limited to, loss of data or interruption of services.

2) MNPS is not responsible for the content of any advice or information received by a user from a source outside MNPS, or any costs incurred as a result of such advice.
3) MNPS will not be responsible for financial obligations incurred or arising through the use of the system by employees.

4) MNPS is not responsible for the communications of individuals utilizing the MNPS network.

5) MNPS will undertake good faith efforts to filter "scam" e-mails. Despite good faith efforts, some "scam" e-mails will inevitably be delivered to MNPS users via e-mail or other means. MNPS users are expected to independently evaluate the legitimacy and merits of any solicitation or offer that they might receive via e-mail or other electronic communication. MNPS will not be responsible for any loss that a user might suffer as a result of a scam transmitted via e-mail or other electronic communication method.

4. Student Specific Policies. The policies enumerated in this section are specific to students and are intended to supplement the general policies listed elsewhere in this policy. These student specific policies 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, CDROM/DVDs, digitized information, communication technologies and Internet access. In general, these responsibilities require efficient, ethical, and legal utilization of all technology resources.

a. MNPS will undertake good faith efforts to filter objectionable material available on sites that can be accessed by MNPS students however, filtering efforts may not completely block objectionable content. Any parent wishing to restrict their children's access to the internet and network are required to complete and sign the technology opt-out form. Failure to complete and sign the technology opt-out form will serve as an indication that your child has permission to access the District's internet and network.

b. 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, online services and/or e-mail use could result in permanent loss of Internet, online services and/or e-mail privileges, and other disciplinary action consistent with the Student Code of Conduct. If a student's misuse of Internet, online services, and/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.

c. Use of Personal Technology and Social Media. Personal technology, blogging, tweeting, texting and personal usage of social media sites (such as, but not limited to, MySpace and Facebook) is not permitted without the express approval of the instructional staff for the course(s) in which a student is enrolled. Further, students are prohibited from posting, using MNPS resources to any internet site outside the official Metro Nashville Public Schools network, or through any electronic media, any material that identifies students or provides any information that would be considered confidential according to the Family Education Rights and Privacy Act (FERPA).

d. Expectations for Use:

    1) A staff member only allows student use of computers, other technology hardware, software, and computer networks, including the Internet, when supervised or granted permission. 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.

    2) 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.

    3) Students who identify or know about a computer security problem or a way of bypassing established filtering and other network security procedures are expected to convey the details to their teacher without discussing it with other students.

    4) Any attempt to alter data, the configuration of a computer, or the files of another user without the consent of that individual, a campus administrator, or

a technology administrator, will be considered an act of vandalism and subject the student to disciplinary action in accordance with the District's Student Code of Acceptable Behavior.

e. Consequences for Misuse

1) The individual to whom computer hardware is issued will be responsible at all times for its appropriate use.

2) Use or possession of hacking software is strictly prohibited and violators will be subject to consequences outlined in the Student Code.

3) 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.

5. Staff Specific Policies. The policies enumerated in this section are specific to staff and are intended to supplement the general policies enumerated elsewhere in this policy. MNPS staff will comply with the following when using MNPS technology resources.

a. MNPS Staff are assigned specific usernames and passwords in order to conduct business on the MNPS network. Any password assigned to a specific user is not to be shared with anyone. If a password is compromised, or if compromise is suspected, the staff member must contact the MNPS helpdesk to change their password as quickly as possible after the discovery.

b. All instructional staff and their supervisors shall be aware of and comply with the Children's Internet Protection Act (CIPA) policy that addresses the five components of responsibility:
   - Access by minors to inappropriate matter on the Internet and World Wide Web
   - The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications
   - Unauthorized access including "hacking" and other unlawful activities by minors online
   - Unauthorized disclosure, use, and dissemination of personal information regarding minors
   - Measures designed to restrict minors' access to materials harmful to minors

Instructional staff shall include in their instruction of the education of minors the appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyber bullying awareness and response.

c. Unauthorized access, including "hacking" is prohibited. Unauthorized tampering with, or access to, the district's student management system that results in changes to student information is unlawful and a violation of the Family Educational Rights and Privacy Act (FERPA, 34 CFR Part 99).

d. 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.

e. Contractors and consultants who have been granted temporary access to the MNPS network shall be governed by the same policy, rules and regulations as MNPS students and staff. Additional restrictions may be imposed when access is given to confidential information.

f. Use of Personal Technology and Social Media. Social media and networking sites may be accessed through the MNPS network for instructional purposes. Blogging, tweeting, texting and using social media sites for personal purposes is limited to duty-free breaks and lunch hours. Further, employees are prohibited from posting (at work or anytime) to any internet site outside the official Metro Nashville Public Schools network, or through any electronic media, any material that identifies students or provides any information that would be considered confidential according to the Family Education Rights and Privacy Act (FERPA) or that otherwise discloses confidential information concerning the district. Employees must prominently disclaim any connection between views expressed on their blog and those of Metro Nashville Public Schools. Additional guidelines and restrictions are included in the Employee Social Media Policy HR 5.114.

g. Consequences for Misuse. Noncompliance with the guidelines published in this or other applicable sections of this policy may result in termination of technology privileges and additional disciplinary actions.

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

Broadband Data Improvement Act (S.1492, Public Act 110-385). Title II **Protecting Children in the 21st Century Act**.
SS 3.122 Information Release Policy (MNPS Policy)
MNPS Student Code of Conduct

The Metropolitan Nashville Public Schools Electronic Media and Telecommunications Networks Use Agreement Form

I hereby agree that I have read the document entitled, "Employee Technology Acceptable Use Policy" and certify that I am familiar with the contents of the document and agree to comply with the terms contained therein. I also acknowledge my understanding that any violations of the Agreement may result in disciplinary action. Disciplinary action may include, but is not limited to, removal of e-mail services, removal of Internet services, suspension or access to computers and networks, suspension of employment, termination of employment, and/or recommendation for prosecution.

User Name (Print):
_____

User Signature:
_____

Date: _____

NOTE: This signed document will be maintained in the employee's employment file (MNPS employees)