RESPONSIBLE USE OF TECHNOLOGY

1. Statement of District Policy.

The MSD of Wayne Township believes accessing content on the Internet is an essential component to prepare students for their life and careers. The goal in providing access to the internet and other technology to staff and students is to promote educational excellence by facilitating collaboration, innovation, and communication. The District believes in freedom and self-regulation and encourages students and staff to use the Internet and technology responsibly. The use of the Internet and technology is a privilege, not a right, and inappropriate use may result in a cancellation of some or all privileges. The District reserves the right to read, print, delete, store, or use any transmission on this system at its discretion and grants permission to use this system for educational purposes only.

2. Scope of this Policy.

This Policy applies to all technology provided by the District as well as the personal devices of students and employees (collectively "Users"). This includes, but is not limited to, telephones, cellular devices, digital media players, tablets, laptop and desktop computers and work stations, direct radio communication, Internet access, voice mail, e-mail, text messaging, facsimile transmission and receipt, and any computer based research and/ or communication.

3. Definition of Terms Used in this Policy.

As used in this Policy:

“Confidential information” means information that is declared or permitted to be treated as confidential by state or federal law, including the Family Educational Rights and Privacy Act (FERPA), or District Policy on access to public records.

“Proprietary information” means information in which a person or entity has a recognized property interest such as a copyright.

"Personal device" includes cell phones, smart phones, laptops, tablets, handhelds or any other device that is not the property of the District but is used at school or a school activity, or connected to District technology by a wired or wireless link.

“Technology" means computers and computer systems, public and private networks such as the Internet, phone networks, cable networks, voice mail, e- mail, telephone systems, copiers, fax machines, audio-visual systems, cellular devices, tablets, laptop and desktop computers, direct radio communications, text messaging, and similar equipment as may become available.

"User" means a District employee, student, volunteer or other person authorized to use District technology.

4. Violation of this Policy.

a. Violations of this Policy may result in denial of further access to technology, suspension or expulsion of students, and discipline of employees including suspension or termination of employment. Such a violation by a person affiliated with a contractor or subcontractor rendering services to the District may result in cancellation of the contract of the contractor or sub-contractor.

b. A User observing or learning of a violation of this policy is required to report the violation of this Policy to the user's immediate supervisor (for employees or volunteers), or to a teacher or other school administrator (for students).

5. Ownership of District Technology & Information.

The technology provided by the District and all information stored by that technology is at all times the property of the District. Documents and other works created or stored on the District technology are the property of the District and are not the private property of the User. This includes all information created using technology and/or placed on a website, blog and/or other storage device.

6. Access to Information and Investigation of Potential Policy Violations.

a. Users shall not have an expectation of privacy in any use of District technology or the content of any communication using that technology, and the IT Services Staff or a designee may monitor their use of technology without notice to them, and examine all system activities the User participates in including but not limited to, e-mail, recorded voice and video transmissions, to ensure proper and responsible use of the District's technology. Monitoring shall include the use of voicemail but shall not include monitoring a live communication between two or more parties unless at least one User is aware of the monitoring. In addition, use of District technology may be subject to production pursuant to the Indiana Access to Public Records Act, Ind. Code 5-14-3.

b. A User's history of use and all data stored on or sent to or from District technology shall at all times be subject to inspection by the IT Services Staff or a designee without notice to the User before or after the inspection.

c. If IT Services Staff has reasonable suspicion to believe a User has violated this policy or additional District rules, the IT Services Staff or a designee may investigate to determine if a violation has occurred. If the investigation is not conducted by the IT the results of the investigation shall be reported to the IT Services Staff by e-mail or in person, and the IT Services Staff shall take appropriate action.

d. A decision by IT Services Staff in response to an investigated allegation of a violation of this policy or additional District rules may be appealed in writing to the Superintendent within five (5) calendar days. The Superintendent's decision concerning continued access to District technology and any other penalty shall be final.

7. Conditions and Standards for Responsible Use of Technology.

a. Responsible use of technology is ethical, academically honest, respectful of the rights of others, and consistent with the District's mission. Technology should be used by students to learn and communicate in correlation with the curriculum while under a teacher or supervisor's direction. Student owned personal devices and District technology shall be used by students under teacher supervision with the purpose of improving instruction and student learning.

b. Users will become familiar with and comply with all expectations of the District for the responsible use of District technology as communicated in school handbooks, school District policy, and other communications and standards concerning the use of District technology.

c. Users must respect and protect the privacy and intellectual property rights of others and the principles of their school community. The IT Services Staff are the only individuals authorized to select, adopt and allow the use of specific web based resources for teacher and student use, including resources for website creation, multimedia projects, presentations, and other collaborations. The IT Services Staff in consultation with the Superintendent's other designees will select resources based upon online safety, coordinated professional development, and informed technical support. If a teacher or student desires to use an alternate resource, they must make a request to the IT Services Staff via the established process. Further, Users shall not alter, delete, or destroy data, information, or programmatic instructions contained in or on District technology without permission from the IT Services Staff. Personally generated files and documents may be deleted by the User who created them, unless they may include proprietary information, a student's personally identifiable information, and/or information potentially subject to litigation.

d. Any recording made on school grounds may be subject to copyright laws (see District policy "Copyrighted Materials") and the protection of the privacy rights of others, including personally identifiable information about a student protected by the Family Education Rights and Privacy Act ("FERPA"). Where IT Services Staff or other District staff have reasonable suspicion that a recording, data, or image was made in violation of this Policy, such item may be confiscated by District staff. Any use of a recording device to invade the privacy of another person will result in sanctions for the person making the recording.

e. Users must notify IT Services Staff if they have violated the conditions established for the use of District technology or have witnessed or become aware of another User misusing District technology. Users shall be responsible for noting and reporting any inappropriate use of District technology in violation of District policy or conduct standards including threats, bullying, harassment, or communications proposing or constituting a violation of the law or the Student Code of Conduct.

f. If a User creates a password, code or encryption device to restrict or inhibit access to electronic mail or files, the User will provide access to that information when requested to do so only by the User's supervisor, teacher, or the IT Services Staff. This includes personal technology brought to or accessed during the work or student day or at a school activity including bus transportation. The IT Services Staff or a designee shall be authorized to override any password, code or encryption device to access the technology. Users shall not use District technology anonymously or use pseudonyms to attempt to escape from responsibilities under this policy, regulations, or the law.

g. Creation of an account, access to a new application, or any other initial use of software or technological applications in the public domain (non-District managed technology) must be under the supervision of a teacher, for instructional purposes, and only on school approved sites.

h. A User shall never use another User's password, or account, even with the permission from the User. Any need to have access to another User's account should be addressed to the IT Services Staff or a designee.

i. An unauthorized attempt to log on to District technology as a System Administrator will result in cancellation of the User's access to District technology and may result in more severe discipline including termination for employees and expulsion for students.

j. Students shall not be required to divulge personal information for access to a non-District managed technology.

k. Students will be permitted access to the Internet through District technology unless a parent/guardian has signed and returned a "Denial of Internet Access Form" within the preceding twelve (12) months.

l. In order to comply with the Children's Internet Protection Act ("CIPA"), the Board has implemented technology protection measures that protect against (e.g., filter or block) access to visual displays/depictions/materials that are obscene, constitute child pornography, and/or are harmful to minors. Thus, Student use shall be filtered to minimize access to inappropriate materials. Student access to inappropriate materials despite the presence of the filter shall be reported immediately to the IT Services Staff. The filtering

software shall not be disabled or circumvented without the written authorization of IT Services Staff or designee.

m. While online, student Users should not reveal personal information such as name, age, gender, home address or telephone number, and are encouraged not to respond to unsolicited online contacts and to report to a teacher or supervisor any online contacts which are frightening, threatening, or otherwise inappropriate.

n. Students, parents and staff are advised that any student connection to any Internet or network provider not under District control may not be filtered to the same degree as connection through District provided access. The District is not responsible for the consequences of access to sites or information through resources that circumvent the District's filtering software.

o. Users accessing the Internet through personal devices connected to District technology must comply with this policy.

p. Users connecting personal devices to District technology do so at their own risk. The District is not responsible for damages to hardware or software as a result of the connection of personal devices to District technology.

q. Users must not knowingly cause damage to District technology, including transmit a computer virus or other malware that is known by the User to have the capability to damage or impair the operation of District technology, or the technology of another person, provider, or organization, nor shall a User take any action that could cause damage to District technology or other District property.

The Superintendent is authorized to develop administrative guidelines further refining what communication is related to District business.

8. Protection of Proprietary and Confidential Information Communicated or Stored on District Technology.

a. Users of the District's technology are expected to protect the integrity of data, personal privacy, and property rights of other persons when using District technology.

b. The practice of using distribution lists to send information shall not excuse the erroneous disclosure of confidential information. Users shall determine that distribution lists are current and review each name on any list before sending confidential information including, but not limited to, personally identifiable information about students protected by the Family Educational Rights and Privacy Act ("FERPA").

c. Users should not access confidential information in the presence of others who do not have authorization to have access to the information. Confidential information should not be left visible on the monitor when a User is away from the monitor.

d. Users should not copy, file share, install or distribute any copyrighted material such as software, database files, documentations, articles, music, video, graphic files, and other information, unless the User has confirmed in advance that the District has a license permitting copying, sharing, installation, or distribution of the material from the copyright owner. Violation of the right of a copyright owner will result in discipline of a student or employee.

9. Incurring Fees for Services.

No User shall allow charges or fees for services or access to a database to be charged to the District except as specifically authorized in advance of the use by IT Services Staff. A fee or charge mistakenly incurred shall be immediately reported to the IT Services Staff. Incurring fees or charges for services to be paid by the District for personal use or without prior authorization of the IT Services Staff may result in discipline including suspension or expulsion of a student, or suspension or termination of an employee.

Users shall thoroughly review terms and conditions of any programs, software, or applications prior to accepting the terms and conditions. Users are responsible for ensuring the terms and conditions comply with District Policy and procedures and state and federal law. Users who are unsure of the terms and conditions shall contact the IT Services Staff prior to accepting any terms and conditions. Accepting terms and conditions that violate District policy or procedures or state or federal law may result in discipline as described below.

10. Liability

Use of Technology is at the User's own risk. The system is provided on an "as is, as available" basis. The District is not responsible for any damage Users may suffer. The District is not responsible for the accuracy or quality of any advice or information obtained through or stored on the District's system, nor is it responsible for damages or injuries from improper communications or damage to property used to access District technology. The District is not responsible for financial obligations arising through unauthorized use of the educational technologies or the Internet.

11. Training

All students and those staff members who work directly with students shall receive annual training on social media safety, cyber bullying, and appropriate responses.

Children's Internet Protection Act (CIPA)

MSD of Wayne Township, Marion County, Indiana

Adopted: January 15, 1996
Revised: April 22, 1996
Revised: July 13, 1998
Revised: July 10, 2000
Revised: October 15, 2001
Revised: November 15, 2010
Revised: September 8, 2014
Revised: December 9, 2019