RESPONSIBLE USE OF TECHNOLOGY AND INTERNET USE POLICY

1. Statement of District Policy:

The Metropolitan School District of Washington Township ("District") believes accessing content on the Internet is essential to fully prepare students for their careers and life. The goal in providing access to the Internet and other technology to staff and students is to promote educational excellence by facilitating instruction, collaboration, innovation, and communication. The District's students and employees (collectively "Users") accessing the Internet are representing the District and therefore have a responsibility to use the Internet in a productive manner that meets the ethical standards of an educational institution.

It is the joint responsibility of students, parents, and employees of the District to assure the appropriate and effective use of technology to both enhance the quality of student learning and the efficiency of District operations. The smooth and reliable operation of the District's technological resources is dependent upon the proper conduct of the end users who must adhere to stated policies.

Use of any and all technological resources is a privilege, not a right, and as such, users take seriously the responsibilities associated with signing the user agreement. The User Agreement is part of the student handbook. Parents digitally acknowledge usage terms in the student information system during annual data cleanup and information updates. Inappropriate use may result in a cancellation of some or all privileges and/or other appropriate discipline. 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 Use:

To ensure that students receive a quality education in an intellectually stimulating environment, both during in-person learning and virtual learning, it is the goal of the District to provide all students with access to a variety of technological resources. All technological resources shall be used in accordance with any and all District policies as well as local, state, and federal laws governing the usage of technology and its component parts. All users shall use the provided technological resources so as not to waste or abuse, interfere with or cause harm to other individuals, institutions, or companies.

This policy applies to all technology provided by the District as well as the personal devices of 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, direct messaging through device applications, facsimile transmission and receipt, artificial intelligence, including language-generation tools and large language models, and any computer based research and/or communication.

3. Definition of Terms Used:

"Confidential information" means information that is declared or permitted to be treated as confidential by state or federal law, including the Family Education Rights and Privacy Act ("FERPA"), or District policy or guideline 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, artificial intelligence, including language-generation tools and large language models, 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, direct messaging through device applications, and similar equipment as may become available.

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

4. Ownership of District Technology and 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.

5. 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 shall NOT use the Network to: Access, create, send or receive, store, or display obscene materials; create or send threatening or libelous communications or communications which include vulgar, abusive, or otherwise inappropriate language; access or use other individuals' accounts, information, or files without permission; access websites, files, or other information or resources using passwords not specifically assigned to themselves; pursue commercial or for-profit endeavors; wantonly waste district resources; damage, disable, or otherwise disrupt the operation of the network; or violate any local, state, or federal statutes, including but not limited to copyright law. Users shall not send, receive, view, or download materials that are harmful to minors, as defined by I.C. 35-49-2-2, on District technology.

d. 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 propriety information, a student's personally identifiable information, and/or information potentially subject to litigation.

e. Any recording made on school grounds or during instructional time, whether in-person or virtual, may be subject to copyright laws 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.

f. 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.

g. 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.

h. 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.

i. 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 shall be addressed with the IT Services Staff or a designee.

j. 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.

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

l. 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.

m. In order to comply with the Children's Internet Protection Act ("CIPA") and I.C. 20-26-5-40.5, 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.

n. The District may utilize a wide variety of third-party web-based applications in its curriculum. Although these applications are widely used by the education community and support K-12 institutions, the terms of service for many sites require explicit parental permission for children under the age of 13. The Children's Online Privacy Protection Rule permits the District to provide the necessary consent for educational purposes.

o. While online, student users shall 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.

p. 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.

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

r. 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.

s. 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.

6. Conditions and Standards for Responsible Use of Electronic Communication:

a. Communications with students/parents/guardians, even if not using school resources, are within the jurisdiction of the District to monitor as they arise out of one's position as an educator. For official District business, employees are to use a District email account when communicating with a student/parent/guardian via email.

b. Electronic communication between staff and students/parents/guardians should be

written as a professional representing the District. This includes word choices, tone, grammar, and subject matter.

c. All data stored or transmitted on District computers shall be monitored. District email accounts shall not be used for sending or attempting to send anonymous messages.

d. Unauthorized photos and videos of students and staff shall not be shared or posted electronically.

e. Electronic correspondence is a public record under the public records law and may be subject to public inspection.

f. The line between professional life and personal life must be clear at all times. District employees should only use their District account or other approved communication method (Google, Zoom, etc.) to communicate with students and/or parents and guardians, and should only communicate on matters directly related to education. Relationships associated with such educational social media accounts should only be with members of the educational community, such as administrators, teachers, students, and parents of such students.

g. All District employees will be responsible for information that they make public through the use of electronic communication. Teachers are the gatekeeper for the privacy and protection of students. When other people can see your conversations with students (i.e. followers on Twitter or friends on Facebook), you may be endangering them and also violating the Family Educational Rights and Privacy Act ("FERPA").

7. Conditions and Standards for Responsible Use of Virtual Instruction:

a. All policies, rules, and applicable state and/or federal law apply when in virtual learning classrooms.

b. All staff and students should conduct themselves as if they are physically present in the classroom.

c. Staff shall password protect all meetings and monitor attendance to ensure privacy.

d. Staff and students shall manage screen sharing options while conducting or participating in class.

e. Staff shall stop class if it is necessary to protect the privacy of a student or a group of students.

f. No individual, including parent(s) or guardian(s), shall record a class session unless it is a staff member and there is an educational reason for doing so and necessary permission has been obtained.

g. If an unauthorized individual is in a session, staff shall direct the outside individual or group to leave the session immediately. If they refuse to do so, staff shall end the class and start a new, private session. If a student notices an unauthorized individual

present in the class, he or she should report that individual to the staff member in the meeting. The staff member should report the intrusion to Administration immediately.

8. Access to Information and Investigation of Potential Violations:

a. The District recognizes it may not be possible to technologically limit all Internet access to only those materials that support and enrich the curriculum according to adopted policies and reasonable selection criteria. For this reason, at the discretion of the District or the Superintendent, technology protection measures may be configured to protect against access to any material considered inappropriate for students to access. Further, the technology protection measures will not purposefully be disabled at any time that students may be using the Network to help protect against access to materials that are prohibited under the Children's Internet Protection Act and/or District policy and guidelines. Any student who attempts to disable the technology protection measures will be subject to discipline. The Superintendent or his designee may temporarily or permanently unblock access to sites containing appropriate material, if access to such sites has been blocked by the technology protection measures. The determination of whether material blocked shall be based on curriculum concerns, including the content of the material and the intended use of the material, policy concerns, network concerns, and safety concerns.

b. 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.

c. 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.

d. 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 IT Services Staff, 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.

e. 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.

9. Violations of Responsible Use of Technology:

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. A violation of this policy by parent(s) or guardian(s) may result in legal measures including, but not limited to, the following measures to ensure the safety and privacy of Users: cease and desist communication and civil or criminal charges.

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

10. Social Media Use:

a. Users' personal or private use of social media, even when occurring off school property and outside school hours, may have unintended consequences that affect the school environment.

b. Social media use should be in a manner sensitive to the Student Code of Conduct and the employees' professional responsibilities.

c. The intent of this policy is not to infringe upon Users' legal rights, such as the freedom of expression, religion, and association. For example, this policy does not prohibit an employee from posting content outside the scope of their employment and on a matter of public concern. However, those rights do not include permission to post inflammatory comments and/or any statements that could compromise the District's mission, constitute cyber-bullying or harassment, or cause a substantial disruption to the school environment.

Violations: Violations of the social media use provision may result in disciplinary action (including expulsion for students or termination for employees), confiscation of the device, loss of use of District technology resources, referral to law enforcement or the Department of Child Services, and the recording, data, or image made in violation may be deleted. If the Superintendent or designee has reasonable suspicion to believe an employee or student has violated this policy or District rules related to technology, they may investigate to determine if a violation occurred.

11. 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.

12. 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 discussed within this policy.

13. 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.

14. Training

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

47 U.S.C. §254(h)(5)(B)-(C), 254(l)
20 U.S.C. §67777(a)
47 C.F.R. §54.520(c)(1)(i)
Children's Internet Protection Act (CIPA)
I.C. 20-26-5-40.5

Metropolitan School District of Washington Township

Adopted: 01/24/24
Revised: [date]