
Student Use of Technology

Mapleton Public Schools (the “District”) believes the Internet, electronic communications, social media, applications, and artificial intelligence tools have vast potential to support instruction and student learning. The Board of Education believes appropriate technology should be used in schools as a learning resource to educate and inform.

Use of technology requires students to think critically, analyze information, write clearly, utilize problem-solving skills, and develop computer and research skills that employers demand. Use of these tools also encourages an attitude of lifelong learning and offers an opportunity for students to participate in distance learning activities, communicate with other students and individuals, and locate information.

Accordingly, the District provides access to technology for students. These resources should be used for educational purposes only while attending school.

Through the use of technology, students may access materials and information from many sources, including some that may be harmful to students. Although it is impossible to predict with certainty what information students might locate or come in contact with, the District will take reasonable steps to protect students from accessing material and information that is obscene, pornographic, or otherwise harmful to minors, as defined by the Board. Students are responsible for their own use of District technology devices to avoid contact with material or information that may be harmful to minors.

For purposes of this policy, “District technology device” means any District-owned computer, hardware, software, or other technology that is used for learning purposes and has access to the Internet.

Blocking or Filtering Obscene, Pornographic, and Harmful Information

Technology that blocks or filters material and information that is obscene, pornographic, or otherwise harmful to minors, as defined by the Board, has been installed on all district computers having Internet and electronic communications access. Students must report access to material and information that is inappropriate, offensive, or otherwise in violation of this policy to a staff member. If a student becomes aware of other students accessing such material or information, they must report it to a staff member.

The District is not capable of preventing students from accessing material and information that is obscene or otherwise harmful to minors on their own personal devices, including cellular telephones. However, accessing such information during the school day, on District grounds, or at a District-sponsored event or activity violates the Student Use of Technology Annual Acceptable Use Agreement (See Exhibit JS-E) and will not be tolerated, whether the student is connected to District Internet, or not. Any student found to be accessing material and information that is obscene or otherwise harmful to minors during the school day, on District grounds, or at a District-sponsored event or activity, even on a personal device, will be subject to disciplinary action.

No Expectation of Privacy

District technology devices are owned by Mapleton Public Schools and are intended to be used for educational purposes at all times. Students shall have no expectation of privacy when using District technology devices, Internet, or electronic communications. Mapleton Public Schools reserves the right to monitor, inspect, copy, review, and store all usage of District technology devices, including all access and transmission/receipt of materials and information via the Internet or electronic communications, at any time and without prior notice. All material and information accessed/received through District technology devices remains the property of Mapleton Public Schools.

Personal Electronic Devices

Students are permitted to bring personal electronic devices to school, subject to the rules of each individual school. Each school is permitted to regulate student access to personal electronic devices during school hours as appropriate.

If a student chooses to bring a personal electronic device to school, on District grounds, or to a District-sponsored event or activity, compliance with this Policy is required. Any conduct on District grounds or at a District-sponsored event or activity that violates this Policy, even if the student is using a personal electronic device, will be subject to disciplinary action, including suspension, expulsion, and/or legal action. The District reserves the right to temporarily confiscate any personal electronic device that is used in violation of this Policy and to prohibit a student from bringing a personal electronic device on District grounds or to District-sponsored events or activities for failure to comply with this Policy.

Unauthorized and Unacceptable Uses

Students must use District technology devices in a responsible, efficient, ethical, and legal manner.

Because technology is constantly changing, it is not possible to specifically describe every unacceptable use of District technology devices. The list below includes examples of unacceptable uses but is by no means exhaustive.

Students must not access, create, transmit, retransmit, or forward material or information that:

- Promotes violence or advocates destruction of property including, but not limited to, access to information concerning the manufacturing or purchasing of destructive devices or weapons;
- Is not related to District educational objectives;
- Contains pornographic, obscene, or other sexually oriented materials, either as pictures or writings;
- Harasses, threatens, demeans, or promotes violence or hatred against another person or group of persons in violation of the District's nondiscrimination policies;
- Is for the purpose of personal profit, financial gain, advertising, commercial transaction, or political purposes ;
- Plagiarizes the work of another;
- Uses inappropriate or profane language;
- Is knowingly false or could be construed as intending to purposely damage another person's reputation;
- Violates any federal or state law, including but not limited to copyrighted material and material protected by trade secret;
- Contains personal information about themselves or others, including information protected by confidentiality laws;
- Impersonates another or transmits through an anonymous remailer; or,
- Accesses fee services without specific permission from the system administrator.

The individual assigned to a District technology device, account, or username is accountable for any and all transactions entered on that District technology device, account, or username.

Security

Security on District technology devices is a high priority. Students who identify a security problem while using a District technology device must immediately notify a staff member or system administrator immediately. Unauthorized attempts to log on to the Internet and electronic communications, as a system administrator are prohibited.

Students must not:

- Use another person's password or any other identifier that was not assigned to them personally by the District;
- Gain or attempt to gain unauthorized access to District technology devices; or,
- Read, alter, delete, copy, or attempt to do any of the above, electronic communications of other system users.

Any user identified as a security risk, or as having a history of problems with technology, may be denied access to the Internet, electronic communications, and/or district technology devices.

Safety

In the interest of student safety, the District will educate students about appropriate online behavior, including cyber-bullying awareness and response, interacting on social media; appropriate use of artificial intelligence, and other forms of direct electronic communications.

In order to protect students' identities and ensure online safety, students must not reveal personal information about themselves or others, such as home address or phone number, while using the Internet or electronic communications. Students must not use their last name or any other information that might allow an individual to locate him or her. Students must not arrange face-to-face meetings with persons met on the Internet or through electronic communications.

Vandalism

Vandalism will result in the cancellation of privileges and may result in legal action and/or disciplinary action, including suspension and/or expulsion, in accordance with Board policy concerning suspension, expulsion, and other disciplinary interventions. Vandalism is defined as any malicious or intentional attempt to harm, destroy, modify, abuse, or disrupt operation of any network within the school district or any network connected to the Internet, operation of any form of electronic communications, the data contained on any network or electronic communications, the data of another user, usage by another user, or district technology device. This includes but is not limited to, the uploading or creation of computer viruses and the use of encryption software.

Artificial Intelligence

The district supports student use of Artificial Intelligence (AI) tools that enhance the district's commitment to high-quality learning. Generally, students may use AI tools for explaining concepts, exploring new topics of interest, and seeking guidance on

research directions. Students may be permitted to use AI tools on assignments if clearly stated in the assignment or specified by the teacher. However, students must not rely solely or primarily on AI tools in completion of coursework unless expressly authorized.

In any use of AI, students should be mindful that AI tools are prone to “hallucinations,” false answers/information, or outdated, misleading, and/or biased information. Thus, students must always verify information provided by AI tools using reliable sources such as textbooks, scientific papers, and reputable educational websites.

Students should not upload or input any personal, confidential, propriety, or sensitive information into any AI tool. Examples include passwords and other personal information such as names, likenesses, social security, credit card, or bank account numbers.

Specific acceptable and unacceptable uses of AI tools may vary based on new technological developments and students must follow the guidance of the district's administrators. Offenses or violations of this Policy will be addressed by the teacher and administrators.

Unauthorized Content

Students are prohibited from using or possessing any software applications, mobile applications, or other content that has been downloaded or is otherwise in the user's possession without appropriate registration and payment of any fees.

Assigning Student Projects and Monitoring Student Use

The District will make reasonable efforts to ensure that District technology devices, the Internet, and electronic communications are used responsibly by students. Administrators, teachers, and staff have a professional responsibility to work together to monitor students' use of District technology, help students develop the intellectual skills needed to discriminate among information sources, to identify information appropriate to their age and developmental levels, and to evaluate and use information to meet educational goals. Students must have specifically defined objectives and search strategies prior to accessing material and information.

Students' use of technology will be supervised by staff. Staff members assigned to supervise student technology use must have received appropriate training in technology safety and monitoring student use.

Opportunities will be made available on a regular basis for parents to observe student use of technology in schools.

Student Use is a Privilege

Use of District technology demands personal responsibility and an understanding of the District's acceptable use policies. Student use of technology is a privilege, not a right, and therefore, can be taken away. Failure to follow the use procedures contained in this policy will result in the loss of the privilege to use these tools and restitution for costs associated with damages, and may result in legal action and/or disciplinary action, including suspension and/or expulsion, in accordance with Board policy concerning suspension, expulsion, and other disciplinary interventions. The District may deny, revoke, or suspend access to District technology devices, the Internet, and electronic communications, and may close student accounts at any time.

Students and their parents/legal guardians are required to complete and sign the District's "Annual Acceptable Use Agreement" at the beginning of each school year (See Exhibit JS-E). Student access will not be permitted until the completed and signed Agreement is received by the school. Completed and signed Agreements shall be retained.

School District Makes No Warranties

Mapleton Public Schools makes no warranties of any kind, whether express or implied, related to the use of District technology devices, including access to the Internet and electronic communications. Providing access to these services does not imply endorsement by Mapleton Public Schools of the content, nor does the District make any guarantee as to the accuracy or quality of information received. The District is not responsible for any damages, losses, or costs a student suffers in using technology. This includes loss of data and service interruptions. Use of any information obtained via technology is at the student's own risk.

Adopted January 22, 2013, by the Board of Education for Mapleton Public Schools.

Revised May 23, 2017.

Revised February 26, 2025.

LEGAL REFERENCES:

20 U.S.C. 6751 et seq. (*Enhancing Education Through Technology Act of 2001*)

47 U.S.C. 254(h) (*Children's Internet Protection Act of 2000*)

47 C.F.R. Part 54, Subpart F (*Universal Support for Schools and Libraries*)

C.R.S. §§ 22-87-101 et seq. (*Children's Internet Protection Act*)

CROSS REFERENCES:

AC: Nondiscrimination/Equal Opportunity

EGAEA: Electronic Communication

JB: Equal Educational Opportunities

JKD/JKE: Suspension/Expulsion of Students

JS-E: Student Annual Acceptable Use Agreement