

## **Student Use of the Internet and Electronic Communications**

Mapleton Public Schools (the “District”) believes the Internet and electronic communications (email, online chat forums, and other forms of electronic communication) have vast potential to support curriculum and student learning and should be used in schools as a learning resource to educate and to inform. Use of the Internet and electronic communications require 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 the Internet and electronic communications for students. These resources should be used for educational purposes only while attending school.

The Internet and electronic communications are fluid environments in which students may access materials and information from many sources, including some that may be harmful to students and to the learning environment. Additionally, the information available online is constantly changing. Accessibility of material or information via the Internet or electronic communications provided by the District does not imply that the District endorses the content. Students shall take responsibility for their own use of District technology devices to avoid contact with material or information that may be harmful to minors, or detrimental to the learning environment.

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 or electronic communications.

### **Blocking or Filtering Obscene, Pornographic, and Harmful Information**

While the District acknowledges that it is impossible to predict with certainty what information students might locate or come in contact with on the Internet, Mapleton Public Schools is committed to taking reasonable steps to protect students from accessing material and information that is obscene or otherwise harmful to minors, as defined by the Board of Education. To this end, the District will install technology that blocks or filters material and information that is obscene or otherwise harmful to minors on each District technology device. Students shall take responsibility for their use of District technology devices to avoid contact with material or information that may be harmful to minors. Students shall be required to report any instances of access to material that is in violation of this Policy to a staff member, including inadvertent access, as well as access by other students.

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 the Internet and Electronic Communications 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. District network administrators may review student files and communications to maintain system integrity and to ensure that users are using the system appropriately and responsibly. 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 shall remain 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. This includes cell phones, tablets, computers, electronic reading devices, watches, and any other electronic device capable of accessing the Internet or displaying content from the Internet. Compliance with this Policy on personal electronic devices is required whether the student is connected to District Internet, or not.

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 shall use District technology devices, the Internet, and electronic communications 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, Internet, and electronic communications. The list below includes examples of unacceptable uses, but is by no means exhaustive. The Board of Education shall have the ultimate word on what constitutes unacceptable use.

No student shall 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, except as provided in other District policies;
- Contains pornographic, obscene, or other sexually oriented materials, either as pictures or writings, which are intended to stimulate erotic feelings or appeal to prurient interests in nudity, sex, or excretion;
- 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 politics;
- Plagiarizes the work of another;
- Uses inappropriate or profane language or depictions likely to offend or intimidate others in the school community;
- 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;
- Uses another individual's Internet or electronic communications account without written permission from that individual;

- 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 are required to notify a staff member or system administrator immediately. Students should not attempt to demonstrate the problem to other users. Unauthorized attempts to log on to the Internet, electronic communications, or a District technology device as a system administrator are prohibited.

Students shall 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.

### **Safety**

In the interest of student safety, the District will take reasonable steps to educate students about appropriate online behavior, including cyber-bullying awareness and response, interacting on social networking sites, and other forms of direct electronic communications.

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

### **Vandalism**

Students are prohibited from performing, or attempting to perform, any action that is intended to harm, destroy, modify, abuse, or disrupt operation of any network within the District or any network connected to the Internet, operation of any form of electronic communications, the data of another user, usage by another user, or District-owned technology device. This includes, but is not limited to, the uploading or creation of computer viruses and the use of encryption software. Vandalism will result in suspension of privileges to access and utilize District technology devices, Internet, and electronic communications, and may result in additional disciplinary action including suspension, expulsion, and/or legal action.

### **Unauthorized Content**

Students are prohibited from using or possessing any software applications, mobile apps, 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 devices, the Internet, and electronic communications, 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 shall have specifically defined objectives and search strategies prior to accessing material and information on the Internet and through electronic communications.

All students shall be supervised by District staff while using the Internet or electronic communications at a ratio of at least one staff member to each 30 students. Staff members assigned to supervise student use shall have received appropriate training in Internet and electronic communications safety and monitoring.

Students may use blogs, wikis, and other forms of collaborative technologies as long as such use is consistent with this Policy, and provided that a staff member is assigned to a moderator role to ensure that inappropriate material is removed in a timely fashion. Neither the school nor the District is responsible for inappropriate content posted by participants acting outside of the identified educational purposes. Use of collaborative technologies with student participation shall be restricted to an environment that includes staff supervision and does not allow anonymous participation. It is acceptable for participants to use screen names as long as the true identity of each student using a

pseudonym is recorded.

Opportunities shall be made available on a regular basis for parents to observe student use of the Internet and electronic communications in schools.

### **Student Use is a Privilege**

Use of District technology devices, the Internet, and electronic communications demands personal responsibility and an understanding of the District's acceptable use policies. Student use of the Internet and electronic communications is a privilege, not a right, and therefore, can be taken away. General rules for behavior apply when using District technology devices, the Internet, and electronic communications. Failure to follow the District's acceptable use policies and procedures will result in disciplinary action, which may include, but is not limited to, loss of the privilege to use District technology devices, the Internet, and electronic communications, suspension, or expulsion. The District may deny, revoke, or suspend access to District technology devices, the Internet, electronic communications, and may close student accounts at any time.

Students and their parents/legal guardians shall be 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 shall not be responsible for any damages, losses, or costs a student suffers in using the Internet and electronic communications including, but not limited to, loss of data and service interruptions. Use of any information obtained via the Internet and electronic communications is at the student's own risk.

*Adopted January 22, 2013, by the Board of Education for Mapleton Public Schools.  
Revised May 23, 2017.*

#### 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