Edina Public Schools
DEFINING EXCELLENCE

Students

~~Internet~~ Electronic Technologies Acceptable Use ~~and Safety Policy~~

I. Purpose

~~The purpose of this policy is to set forth policies and guidelines for access to the school district computer system and acceptable and safe use of the Internet, including electronic communications.~~ This policy sets forth parameters and guidelines for access to the school district's electronic technologies, use of the Internet, use of personal electronic devices on the district's network or connected to district softwares, electronic communications, use of the district's network, Internet, and social networking tools.

II. General Statement of Policy

In making decisions regarding student and employee access to the school district computer system and the Internet, including electronic communications, the ~~school~~ district considers its own stated educational mission, goals, and strategic directions ~~objectives~~. Technology skills are ~~now~~ fundamental to the preparation of citizens and future employees. Access to the district computer system and to the Internet enables students and employees to explore ~~thousands of~~ countless libraries, web pages, databases, ~~bulletin boards,~~ and other resources while exchanging messages with people around the world. The district expects that ~~faculty~~ employees will blend thoughtful use of the district computer system and the Internet throughout the curriculum and will provide guidance and instruction to students in their use.

III. Definitions

A. "Harmful to minors" means any picture, image, graphic image file, or other visual depiction that:

1. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; or

2. Depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and

3. Taken as a whole, lacks serious literary, artistic, political, or

scientific value as to minors.

B. "School-issued device" means hardware or software that the school district, acting independently or with a technology provider, provides to an individual student or employee for that student's or employee's dedicated personal use. A school-issued device includes a device issued through a one-to-one program.

C. "Social Media" refers to any website and application that enables users to create and share content or to participate in social networking. For reference in this policy, social media does not refer to any learning management system (Schoology or Seesaw) or content management systems (Google Workspace).

D. "Technology provider" means a person who:

1. contracts with the ~~school~~ district, as part of a one-to-one program or otherwise, to provide a school-issued device for student use; and

2. creates, receives, or maintains educational data pursuant or incidental to a contract with the ~~school~~ district.

III. Limited Educational Purpose

The school district is providing students and employees with access to the district computer system, which includes Internet access. The purpose of the system is more specific than providing students and employees with general access to the Internet. The Internet is accessible in the district for use as an educational resource. ~~The district system has a limited educational purpose, which includes use of the system for classroom activities, educational research, and professional or career development activities~~. Users are expected to use Internet access through the district system to further educational and personal goals consistent with the mission of the district and school policies. Uses which might be acceptable on a user's private personal account on another system may not be acceptable on this limited-purpose network.

IV. Use of System is a Privilege

The use of the school district system and access to use of the Internet is a privilege, not a right. Depending on the nature and degree of the violation and the number of previous violations, unacceptable use of the district system or the Internet may result in one or more of the following consequences: suspension or cancellation of use or access privileges; payments for damages and repairs; discipline under other appropriate district policies, including suspension, expulsion, exclusion, or termination of employment; or civil or criminal liability under other applicable laws.

Electronic technologies are assets of the district and are protected from unauthorized access, modification, destruction, or disclosure. Use of personal devices, while on district property, is subject to all policies and guidelines, as applicable, plus any state and federal laws related to Internet use, including copyright laws.

V. Unacceptable Uses

A. While not an exhaustive list, ~~T~~the following uses of the school district system and Internet resources or accounts are considered unacceptable:

1. Users will not use the district system to create, record, access, review, upload, download, store, print, post, receive, transmit, or distribute:

a. Pornographic, obscene, or sexually explicit material or other visual depictions;

b. Obscene, abusive, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful, or sexually explicit language or images;

c. Materials that use language or images that are inappropriate in the education setting or disruptive to the educational process;

d. Materials that use language or images that advocate violence or discrimination toward other people, or that may constitute harassment~~,~~ or discrimination, or that threatens the safety of others;

e. Orders for shopping online during time designated as work or academic time by the district; ~~and~~

f. Storage of personal photos, videos, music, or files not related to educational ~~and~~ or extra-curricular purposes for any length of time~~.~~; and

2. Use of social media for non-academic purposes

a. Students age 13 and above may engage in social media as it is connected to extra-curricular or co-curricular activities, and for academic purposes.

b. Per federal law, students under the age of 13 will not be encouraged or required to create accounts or participate in social media, including for academic or extra-curricular purposes.

~~2~~ 3. Users will not use the district system to knowingly or recklessly post, transmit, or distribute false or defamatory information about a person or organization, or to harass another person, or to engage in personal attacks, including prejudicial or discriminatory attacks. This prohibition includes using any technology or other electronic communication off school premises to the extent that student learning or the school environment is substantially and materially disrupted.

~~3~~ 4. Users will not use the district system to engage in any illegal act or violate any local, state, or federal statute or law.

~~4~~ 5. Users will not use the district system to vandalize, damage, or disable the property of another person or organization; will not make deliberate attempts to degrade or disrupt equipment, software, or system performance by spreading computer viruses, engaging in "spamming," or by any other means; will not tamper with, modify, or change the district system software, hardware, or wiring; will not ~~or~~ take any action to violate the district's security system; and will not use the district system in such a way as to disrupt the use of the system by other users.

~~5~~ 6. Users will not use the district system to gain unauthorized access to information resources, or to access another person's materials, information, or files without the direct permission of that person. Users will not attempt to log in through another person's account, or use computer accounts, access codes, or network identification other than those assigned to the user. This clause is not applicable to district technology staff who need to access a system due to a threat, troubleshooting, diagnosing issues, or other IT-related needs that uphold this and other district policies.

7. Individual passwords for computers are confidential and must not be shared.

~~6~~ 8. Users will not use the district system to post or share private information about another person, personal contact information about themselves or other persons, or other personally identifiable information, including, but not limited to, addresses, telephone numbers, school addresses, work addresses, identification numbers, account numbers, access codes or passwords, labeled photographs, or other information that would make the individual's identity easily traceable, and will not repost a message that was sent to the user privately without permission of the person who sent the message.

a. This paragraph does not prohibit the posting of employee contact information on district webpages or communications between employees and other individuals when such communications are made for education-related purposes (i.e., communications with parents/guardians or other staff members related to students). Refer to Policy 515 (Protection and Privacy of Student Records) for direction on directory information for students and how this can be used.

b. Employees creating or posting school-related webpages may include personal contact information about themselves on a webpage. However, employees may not post personal contact information or other personally identifiable information about students unless:

(1) such information is classified by the district as directory information and verification is made that the district has not received notice from a parent/guardian or eligible student that such information is not to be designated as directory information in accordance with ~~Policy 515~~ district policy; or

(2) such information is not classified by the district as directory information but written consent for release of the information to be posted has been obtained from a parent/guardian or eligible student in accordance with ~~Policy 515~~ district policy.

~~In addition, prior to posting any personal contact or personally identifiable information on a school-related webpage, employees shall obtain written approval of the content of the postings from the building administrator.~~

c. These prohibitions specifically prohibit a user from utilizing the district system to post personal information about a user or another individual on social networks, including, but not limited to, social networks such as "Facebook," "X" (formerly called "Twitter~~,~~"), "Instagram," "Snapchat," "TikTok," ~~and~~ "Reddit," and similar websites or applications.

9. Users, outside of IT staff, must not deliberately or knowingly delete a student or employee file, email, or stored information.

7. ~~Users must keep all account information and passwords on file with the designated district official. Users will not attempt to gain unauthorized access to the district system or any other system through the district system, attempt to log in through another~~

~~person's account, or use computer accounts, access codes, or network identification other than those assigned to the user. Messages and records on the district system may not be encrypted without the permission of appropriate school authorities.~~

~~8~~ 10. Users will not use the district system to violate copyright laws or usage licensing agreements, or otherwise to use another person's property without the person's prior approval or proper citation, including the downloading or exchanging of pirated software or copying software to or from any school computer, and will not plagiarize works they find on the Internet.

~~9~~ 11. Users will not use the district system for conducting business, for unauthorized commercial purposes, or for financial gain unrelated to the mission of the district. Users will not use the district system to offer or provide goods or services or for product advertisement. Users will not use the district system to purchase goods or services for personal use without authorization from the appropriate district official.

10. ~~Users will not use the district system to engage in harassment, bullying, or cyberbullying in violation of district policy. the district's Policy 514 (Bullying Prohibition) Policy (Policy 514). This prohibition includes using any technology or other electronic communication off school premises to the extent that student learning or the school environment is substantially and materially disrupted.~~

B. A student or employee who engages in the foregoing unacceptable uses of the Internet or district equipment when they are off district premises may be in violation of this policy, in addition to other district policies. Regardless of whether district equipment was used for the unacceptable use, the district has the right and may be obligated to regulate the off-campus speech or conduct of its students or employees when that speech or conduct materially disrupts the school environment, involves substantial disorder, or constitutes an invasion of the rights of others. Examples of such violations include, but are not limited to, where the ~~school~~ district system is compromised or if a ~~school~~ district employee or student is negatively impacted. If the district receives a report of an unacceptable use originating from a non-school computer or resource, the district may investigate such reports to the best of its ability. Students or employees may be subject to disciplinary action for such conduct, including, but not limited to, suspension or cancellation of the use or access to the district computer system and the Internet and discipline under other appropriate district policies, including suspension, expulsion, exclusion, or termination of employment.

C. If a user inadvertently accesses unacceptable materials or an

unacceptable Internet site, the user ~~shall~~ will immediately disclose the inadvertent access to an appropriate ~~school~~ district official. In the case of a district employee, the immediate disclosure ~~shall~~ will be to the employee's immediate supervisor and/or the building administrator. This disclosure may serve as a defense against an allegation that the user has intentionally violated this policy.

VI. Filter

~~Alternative No. 1~~

A. With respect to any of its computers with Internet access, the school district will ~~monitor~~ filter the online activities of both minors and adults and employ technology protection measures during any use of such computers by minors and adults. The technology protection measures utilized will block or filter Internet access to any visual depictions that are:

1. Obscene;

2. Child pornography; or

3. Harmful to minors.

~~B. The term "harmful to minors" means any picture, image, graphic image file, or other visual depiction that:~~

~~1. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; or~~

~~2. Depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and~~

~~3. Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.~~

~~C~~B. Software filtering technology ~~shall~~ will be narrowly tailored and ~~shall~~ will not discriminate based on viewpoint.

~~D~~C. An administrator, supervisor, or other person authorized by the ~~S~~superintendent may disable the technology protection measure, during use by an adult, to enable access for bona fide research or other lawful purposes.

~~E~~D. The ~~school~~ district will educate students about appropriate online behavior, including interacting with other individuals on social networking

websites and in chat ~~rooms~~ -enabled environments and cyberbullying awareness and response.

VII. Consistency with Other School District Policies

Use of the school district computer system and use of the Internet ~~shall~~ will be consistent with district policies and the mission of the district.

VIII. Limited Expectation of Privacy

A. By authorizing use of the school district system, the district does not relinquish control over materials on the system or contained in files on the system. Users should expect only limited privacy in the contents of personal files on the district system.

B. Routine maintenance and monitoring of the ~~school~~ district system may lead to a discovery that a user has violated this policy, another district policy, or the law.

C. An individual investigation or search will be conducted if ~~school~~ district authorities have a reasonable suspicion that the search will uncover a violation of law or district policy.

D. Parents/guardians have the right at any time to investigate or review the contents of their child's files and ~~e-mail~~ email files in accordance with ~~the school~~ district~~'s Protection and Privacy of Pupil Records P~~policy. ~~515~~ Parents/guardians have the right to request the termination of their child's individual account at any time.

E. ~~School d~~District employees should be aware that the district retains the right at any time to investigate or review the contents of their files and ~~e-mail~~ email files. In addition, district employees should be aware that data and other materials in files maintained on the district system may be subject to review, disclosure, or discovery under ~~Minn. Stat. Ch. 13 (~~the Minnesota Government Data Practices Act~~)~~.

F. The ~~school~~ district will cooperate fully with local, state, and federal authorities in any investigation concerning or related to any illegal activities or activities not in compliance with district policies conducted through the district system.

IX. Internet Use Agreement

A. The proper use of the Internet, and the educational value to be gained from proper Internet use, is the joint responsibility of students, parents/guardians, and employees of the school district.

B. This policy requires the permission of and supervision by the ~~school's~~ district's designated professional staff before a student may use a ~~school~~ district account or resource to access the Internet.

C. The Internet Acceptable Use Agreement form for students must be read and signed by the user~~,~~ and the parent/ ~~or~~ guardian~~, and the supervising teacher~~. This form is signed annually via the Parent Portal. The Internet Acceptable Use Agreement form for employees must be signed by the employee. The form must then be filed at the school office or with a department supervisor. ~~As supervising teachers change, the agreement signed by the new teacher shall be attached to the original agreement.~~

X. Guest Access and Internet Use

A. Guest access to the school district's open wireless network is provided as a service to the community, and is subject to all district policies and guidelines, plus any state and federal laws related to Internet use, including copyright laws. See Appendix VII, Personal Device Access.

B. Guest access provides limited bandwidth, filtered for the following services:

1. Web access (http and https)
2. Email services (pop, imap)
3. Virtual private network services (VPN)

C. Limited technical support is provided for guest access and is identified in the service level agreement found on the district technology website.

XI. Limitation on School District Liability

Use of the school district system is at the user's own risk. The system is provided on an "as is, as available" basis. The district will not be responsible for any damage users may suffer, including, but not limited to, loss, damage, or unavailability of data stored on ~~school~~ district ~~diskettes,~~ cloud services, tapes, hard drives, or servers, or for delays or changes in or interruptions of service or misdeliveries or nondeliveries of information or materials, regardless of the cause. The district is not responsible for the accuracy or quality of any advice or information obtained through or stored on the district system. The district will not be responsible for financial obligations arising through unauthorized use of the district system or the Internet.

XII. User Notification

A. All users ~~shall~~ will be notified of the school district policies relating to Internet use.

B. This notification ~~shall~~ will include the following:

1. Notification that Internet use is subject to compliance with ~~school~~ district policies.

2. Disclaimers limiting the district's liability relative to:

   a. Information stored on district ~~diskettes~~ cloud services, tapes, hard drives, or servers.

   b. Information retrieved through district computers, networks, or online resources.

   c. Personal property used to access district computers, networks, or online resources.

   d. Unauthorized financial obligations resulting from use of district resources/accounts to access the Internet.

3. A description of the privacy rights and limitations of ~~school~~ district sponsored/managed Internet accounts.

4. Notification that, even though the district may use technical means to limit student Internet access, these limits do not provide a foolproof means for enforcing the provisions of this acceptable use policy.

5. Notification that goods and services can be purchased over the Internet that could potentially result in unwanted financial obligations, and that any financial obligation incurred by a student through the Internet is the sole responsibility of the student and/or the student's parents/guardians.

6. Notification that the collection, creation, reception, maintenance, and dissemination of data via the Internet, including electronic communications, is governed by district policy. ~~Policy 406, (Public and Private Personnel Data), and Policy 515, (Protection and Privacy of Pupil Records).~~

7. Notification that, should the user violate the district's acceptable use policy, the user's access privileges may be revoked, school disciplinary action may be taken, and/or appropriate legal action may be taken.

8. Notification that all provisions of the acceptable use policy are subordinate to local, state, and federal laws.

XIII. Parents'/Guardians' Responsibility; Notification of Student Internet Use

A. Outside of school, parents/guardians bear responsibility for the same guidance of Internet use as they exercise with information sources such as television, telephones, radio, movies, and other possibly offensive media. Parents/guardians are responsible for monitoring their student's use of the school district system and of the Internet if the student is accessing the district system from home or a remote location.

B. Parents/guardians will be notified that their students will be using ~~school~~ district resources/accounts to access the Internet and that the district will provide parents/guardians the option to request alternative activities not requiring Internet access. This notification should include:

1. A copy of the user notification form provided to the student user.

2. A description of parent/guardian responsibilities.

3. A statement that the Internet Acceptable Use Agreement must be signed by the user~~,~~ and the parent/~~ or~~ guardian~~, and the supervising teacher~~ prior to use by the student.

4. A statement that the district's acceptable use policy is available for parental/guardian review.

XIV. Notification Regarding Technology Providers

A. Within 30 days of the start of each school year, the school district will give parents/guardians and students direct and timely notice, by United States mail, e-mail, or other direct form of communication, of any curriculum, testing, or assessment technology provider contract affecting a student's educational data. The notice will:

1. identify each curriculum, testing, or assessment technology provider with access to educational data;

2. identify the educational data affected by the curriculum, testing, or assessment technology provider contract; and

3. include information about the contract inspection and provide contact information for a school department to which a parent/guardian or student may direct questions or concerns regarding any program or activity that allows a curriculum, testing, or assessment technology provider to access a student's educational data.

B. A contract between a technology provider and the district will include requirements to ensure appropriate security safeguards for

educational data. The contract will require that:

1. the technology provider's employees or contractors have access to educational data only if authorized; and

2. the technology provider's employees or contractors may be authorized to access educational data only if access is necessary to fulfill the official duties of the employee or contractor.

C. Upon request, the district will provide parents/guardians and students an opportunity to inspect a complete copy of any contract with a technology provider.

D. All educational data created, received, maintained, or disseminated by a technology provider pursuant or incidental to a contract with the district are not the technology provider's property.

XV. School-Issued Devices

A. Except as provided in paragraph B, the school district or a technology provider will not electronically access or monitor:

1. any location-tracking feature of a school-issued device;

2. any audio or visual receiving, transmitting, or recording feature of a school-issued device; or

3. student interactions with a school-issued device, including but not limited to keystrokes and web-browsing activity.

B. The district or a technology provider may only engage in activities prohibited by paragraph A if:

1. the activity is limited to a noncommercial educational purpose for instruction, technical support, or exam-proctoring by district employees, student teachers, staff contracted by the district, a vendor, or the Minnesota Department of Education, and notice is provided in advance;

2. the activity is permitted under a judicial warrant;

3. the district is notified or becomes aware that the device is missing or stolen;

4. the activity is necessary to respond to an imminent threat to life or safety and the access is limited to that purpose;

5. the activity is necessary to comply with federal or state law; or

6. the activity is necessary to participate in federal or state funding programs, including but not limited to the E-Rate program.

C. If the district or a technology provider interacts with a school-issued device as provided in paragraph ~~C~~ B, clause 4, it will, within 72 hours of the access, notify the student to whom the school-issued device was issued or that student's parent/guardian. Such notice will include a written description of the interaction, including which features of the device were accessed and a description of the threat. In the instance in which notification would pose a threat to life or safety, notification will instead be given within 72 hours following the resolution of the imminent threat.

XVI. Use of Email

The school district provides access to electronic mail for district communication between district employees and students, families, and community.

1. The email system will not be used for outside business ventures or other activities that conflict with school board policy.

2. All emails received by, sent through, or generated by computers using the district network are subject to review by the district.

3. Appropriate language must be used when communicating using the district email system or network.

4. All emails are assumed to be documents that can be disclosed to the public unless the content of the email is protected as private or confidential information under data privacy laws. All information contained in an email must be treated in accordance with district policy, regarding student and employee data privacy.

5. Employees will report inappropriate emails to the media specialist, the employee's supervisor, or the director of media and technology services.

6. Emails having content governed by the district's record retention schedule must be kept in accordance with the retention schedule adopted pursuant to Policy 719 (Records Retention).

XVII. Cell Phone Use

A. Students are prohibited from using a cell phone or other electronic communication device to engage in conduct prohibited by school district policies including, but not limited to, cheating, bullying, harassment, and malicious and sadistic conduct.

B. If the district has a reasonable suspicion that a student has violated a district policy, rule, or law by use of a cell phone or other electronic communication device, the district may search the device. The search of the device will be reasonably related in scope to the circumstances justifying the search.

C. Students who use an electronic communication device during the school day and/or in violation of district policies may be subject to disciplinary action pursuant to the district's discipline policy. In addition, a student's cell phone or electronic communication device may be confiscated by the district and, if applicable, provided to law enforcement. Cell phones or other electronic communication devices that are confiscated and retained by the district will be returned in accordance with school building procedures.

XVIII. Limit on Screen Time for Children in Preschool and Kindergarten

A child in a publicly funded preschool or kindergarten program may not use an individual-use screen, such as a tablet, smartphone, or other digital media, without engagement from a teacher or other students. This section does not apply to a child for whom the district ~~school~~ has an individualized family service plan, an individualized education program, or a 504 plan in effect.

~~XIII~~ XIV. Implementation; Policy Review

A. The school district administration may develop appropriate user notification forms, guidelines, and procedures necessary to implement this policy for submission to the school board for approval. ~~Upon approval by the school board, such guidelines, forms, and procedures shall be an addendum to this policy.~~

B. The administration ~~shall~~ will revise the user notifications, including student and parent/guardian notifications, if necessary, to reflect the adoption of these guidelines and procedures.

C. The district Internet policies and procedures are available for review by all parents~~,~~ /guardians, staff, and members of the community.

D. ~~Because of the rapid changes in the development of the Internet, the school board shall conduct an annual review of this policy.~~

Legal References:
Minn. Stat. Ch. 13 (Minnesota Government Data Practices Act)
15 U.S.C. § 6501 *et seq.* (Children's Online Privacy Protection Act)
17 U.S.C. § 101 *et seq.* (Copyrights)

20 U.S.C. § 1232g (Family Educational Rights and Privacy Act)
20 U.S.C. § 6751 *et seq.* (Enhancing Education Through Technology Act of 2001)
47 U.S.C. § 254 (Children's Internet Protection Act of 2000 (CIPA)
47 C.F.R. § 54.520 (FCC rules implementing CIPA)
Minn. Stat. § 121A.031 (School Student Bullying Policy)
Minn. Stat. § 125B.15 (Internet Access for Students)
Minn. Stat. § 125B.26 (Telecommunications/Internet Access Equity ~~Act~~ Aid)*v B.L.,* 594 U.S., 141 S. Ct. 2038 *(2021)*
Tinker v. Des Moines Indep. Cmty. Sch. Dist., 393 U.S. 503 (1969)
United States v. American Library Association, 539 U.S. 194 (2003)
Sagehorn v. Indep. Sch. Dist. No. 728, 122 F.Supp.2d 842 (D. Minn. 2015)
R.S. v. Minnewaska Area Sch. Dist. No. 2149, 894 F.Supp.2d 1128 (D. Minn. 2012)
Tatro v. Univ. of Minnesota, 800 N.W.2d 811 (Minn. App. 2011), aff'd on other grounds 816 N.W.2d 509 (Minn. 2012)
S.J.W. v. Lee's Summit R-7 Sch. Dist., 696 F.3d 771 (8th Cir. 2012)
Parents, Families and Friends of Lesbians and Gays, Inc. v. Camdenton R-III Sch. Dist., 853 F.Supp.2d 888 (W.D. Mo. 2012)
M.T. v. Cent. York Sch. Dist., 937 A.2d 538 (Pa. Commw. Ct. 2007)

Cross References:
~~MSBA/MASA Model~~ Policy 403 (Discipline~~, Suspension, and Dismissal~~ of School District Employees)
~~MSBA/MASA Model~~ Policy 406 (Public and Private Personnel Data)
Policy 413 (Harassment and Violence Prohibition, Students and Employees)
~~MSBA/MASA Model Policy 505 (Distribution of Nonschool-Sponsored Materials on School Premises by Students and Employees)~~
~~MSBA/MASA Model~~ Policy 506 (Student Discipline)
~~MSBA/MASA Model~~ Policy 514 (Bullying Prohibition ~~Policy~~)
~~MSBA/MASA Model~~ Policy 515 (Protection and Privacy of ~~Pupil~~ Student Records)
~~MSBA/MASA Model~~ Policy 519 (~~Interviews of~~ Student~~s~~ Interviews by Outside Agencies)
~~MSBA/MASA Model~~ Policy 521 (Student Disability Nondiscrimination)
~~MSBA/MASA Model~~ Policy 522 (Title IX Sex Nondiscrimination Policy, Grievance Procedure~~s~~ and Process)
Policy 601 (Educational Competencies, Academic Standards and Instructional Curriculum)
~~MSBA/MASA Model~~ Policy 603 (Curriculum and Program Review and Development)
~~MSBA/MASA Model Policy 604 (Instructional Curriculum)~~
~~MSBA/MASA Model~~ Policy 606 (Selection and Review of Text~~books~~, ~~and Instructional~~ Materials, Content or Issues)
Policy 622 (Copyright Policy)
~~Policy 634 (Electronic Technologies Acceptable Use)~~
~~MSBA/MASA Model~~ Policy 806 (~~Crisis~~ Emergency Management ~~Policy~~)
~~MSBA/MASA Model~~ Policy 904 (Distribution or Display of Materials on School District Property by ~~Nonschool~~ Nondistrict Persons or Organizations)

Appendix I to ~~Policy 634~~ Policy 524

STUDENT ONLINE ACCEPTABLE USE CONSENT FORM

Student

By signing below, I agree to follow Edina Public Schools' Electronic Technologies Acceptable Use policy. I understand that my use of the network is a privilege and requires proper online ~~etiquette~~ responsibility. I further understand that misuse of the network will result in disciplinary action.

Student Name (PRINT) _____

Student I.D. Number _____
(MIDDLE SCHOOLS AND HIGH SCHOOL ONLY)

Student Signature _____
(MIDDLE SCHOOLS AND HIGH SCHOOL ONLY)

Address _____ Zip _____

~~Telephone Number _____~~

School Building _____

Parent or Guardian

I give permission for my child to have access to the Internet using the district's computer network. I also understand that some material accessible through the interconnected systems may be inappropriate for school-age students. I agree to defend, indemnify, and hold harmless Edina Public Schools from any and all claims arising out of or related to the use of this interconnected computer system. I further understand that I have the right to withdraw my approval in writing at any time.

☐ Approved

☐ Disapproved

Parent/Guardian Name (PRINT) _____

Signature of Parent/Guardian _____

Date _____

This form ~~can~~ should be completed electronically through the online portal~~, or return this form to your school.~~

Revised: 9/24/12
Modified: 10/13/17
Reviewed: 4/20/20
Reviewed: 8/8/22

Appendix II to ~~Policy 634~~ Policy 524

STUDENT ONLINE CODE OF ETHICS

In the Edina Public Schools, it is important to use information and technology in safe, legal, and responsible ways. At the same time, the school district has a desire for our students to leave our system with a "positive digital footprint," ~~so that employers and post-secondary institutions can see the great work that they have done~~. We embrace these conditions as facets of being a digital citizen and strive to help students develop a positive digital footprint.

1. Students accessing or using electronic products, including but not limited to blogs, wikis, podcasts, Google ~~applications~~ workspace, and district learning management systems for student assignments are required to keep personal information out of their postings.

   At the high school level, parents/guardians may opt to allow their students to utilize their full name in order to increase their positive digital footprint when publishing to an authentic audience.

2. Students will select online names that are appropriate and will consider the information and images that are posted online at an age-appropriate level.

3. Students will not log in to the network, devices, or other educational technologies as another classmate.

4. Students using electronic tools will treat these tools as a classroom space. Speech that is inappropriate for class is not appropriate on electronic tools. Students are expected to treat others and their ideas online with respect.

5. Assignments on electronic tools are like any other assignment in school. Students, in the course of completing the assignment, are expected to abide by policies and procedures in the student handbook, including those policies regarding plagiarism, academic ~~dishonesty~~ integrity, and acceptable use of technology.

6. Student blogs, webpages, and other content creation tools are to be a forum for student expression; however, they are first and foremost a tool for learning. The district may restrict speech for valid educational reasons as outlined in school board policy.

7. Students will not use the Internet, in connection with the teacher assignments, to harass, discriminate, bully, or threaten the safety of others. If students receive a comment on an electronic tool used in school that makes them feel uncomfortable or is not respectful, they must report this to a teacher or another trusted staff member, and must not respond to the comment. Student conduct that occurs off-campus, but has a connection to the school environment, may form the basis for school discipline. This specifically includes activities that occur off-campus over the internet, on social media, or through other communications.

8. Students accessing electronic tools from home or school, using school equipment, will not download or install any software without permission, and will not click on ads or unknown links. ~~competitions.~~

9. Students should be honest, fair, and ~~courageous~~ show integrity in gathering, interpreting, and expressing information for the benefit of others. Always identify sources and test the accuracy of information from all sources.

10. Students will treat information, sources, subjects, colleagues, and information consumers as people deserving of respect. Gathering and expressing information should never cause harm or threaten to be harmful to any person or group of people. Students will gain permission from students or staff who are the focus of their research, recording, or content creation.

11. Students are accountable to their readers, listeners, and viewers, and to each other. Admit mistakes and correct them promptly. Expose unethical information and practices of others.

12. Users will not repost or resend content that was sent to the user privately without the permission of the person who created the content.

13. ~~School b~~ Board policies concerning acceptable use of electronic technology include the use of these electronic tools for school activities (Policy 524 - Electronic Technologies Acceptable Use, Policy 622 - Copyright Policy~~, and Policy 634 - Electronic Technologies Acceptable Use).~~

14. Failure to follow this code of ethics will result in academic sanctions and/or disciplinary action.

Revised: 9/24/12
Modified: 11/13/17
Reviewed: 4/20/20
Revised: 8/8/22

Appendix III to ~~Policy 634~~ Policy 524

GUIDELINES FOR EMPLOYEE'S PERSONAL USE OF SOCIAL NETWORKING

The decision to use online social networking for personal use is at the employee's discretion. The school district does not affirmatively monitor employee use of non-district, online social networking tools if the employee is not using district electronic technologies; however, the district may take appropriate action when it becomes aware of, or suspects, conduct or communication on an online social media site that adversely affects the workplace or violates applicable professional codes of ethics. These guidelines are for employees engaging in social networking for personal use.

1. When using your personal social networking sites, refrain from fraternization with students.

2. Ensure that social networking postings are appropriate for the public.

3. Weigh whether a posting will put your effectiveness as an employee at risk.

4. Use caution with regard to exaggeration, profanity, guesswork, copyrighted materials, legal conclusions, and derogatory comments.

5. Ensure compliance with data privacy laws and district policies. Employees will be held responsible for inappropriate disclosure, whether purposeful or inadvertent.

2. Respect your coworkers and students. Do not discuss students, their families, or coworkers.

3. Student images obtained from your employment with the district should not be included on personal social networking sites.

4. Set privacy settings carefully to ensure that you know who has access to the content on your social networking sites.

5. If the public may consider your statements to be made in your capacity as a district employee, you may want to include "This posting is my own and does not represent the view of Edina Public Schools." An employee in a leadership role in the district, by virtue of their position, must consider whether personal thoughts ~~he or she~~ they publish~~es~~ will be attributed to the district. The use of the aforementioned phrase does not preclude the employee from disciplinary action.

6. Social media identifications, login identifications, and user names must not contain the district's name or logo without prior written permission from (1) the ~~D~~director of ~~M~~media and ~~T~~technology ~~S~~services ~~and (2)~~ or to the ~~D~~director of ~~M~~marketing and ~~C~~communications.

Appendix IV to ~~Policy 634~~ Policy 524

GUIDELINES FOR CLASSROOM USE OF SOCIAL MEDIA TOOLS

~~The district provides teachers with password-protected, online social media tools that can be used for instruction. teacher~~ Staff members may ~~also~~ elect to use ~~other~~ social media tools for the purpose of instruction in accordance with Policy 524 ~~634 (Electronic Technologies Acceptable Use) and its appendices. .~~

A. District Online Social Media Tools

1. Content and use must adhere to district policies and guidelines.

2. The platform for instruction must indicate that views expressed on the social media site are that of the employee or student, and do not necessarily reflect the views of Edina Public Schools.

3. The ~~teacher~~ staff member must not disclose information on any online social media site that is district property, protected by data privacy laws, or in violation of copyright.

B. Non-district Social Media Tools

1. If a ~~teacher~~ staff member elects to use a non-district social media tool, the ~~teacher~~ staff member must build a separate page in that social media tool from their personal online presence.

2. Content and use must adhere to district policies and guidelines.

3. Content and use must not violate the “terms of service” for the social media tool.

4. The platform for instruction must indicate that views expressed on the social media site are that of the employee or student, and do not necessarily reflect the views of Edina Public Schools.

5. The ~~teacher~~ staff member must not disclose information on any online social media site that is district property, protected by data privacy laws, or in violation of copyright.

6. The platform must not use official district or school logos without the permission of (1) the ~~D~~director of ~~M~~media and ~~T~~technology ~~S~~services ~~and (2)~~ or the ~~D~~director of ~~M~~marketing and ~~C~~communications.

Appendix V to ~~Policy 634~~ Policy 524

GUIDELINES FOR SCHOOL OR DISTRICT USE OF SOCIAL MEDIA TOOLS

Individual schools and departments may choose to establish an official presence on public online social media sites with prior administrative approval. A request must contain the following information:

1. Sponsoring school or department;
2. Proposed social media site or other location;
3. Purpose of site, which cannot be served by the current district website;
4. Plan on how to comply with district policies and record retention requirements;
5. Description and primary use of site;
6. Plan for monitoring site, addressing policy violations, and ensuring current content; and
7. Designee for maintaining the site.

The request should be submitted to the ~~Ddirector of Mmedia and Ttechnology Sservices~~ Director of Marketing and Communications. Written approval or denial will be provided to the school or department. If the request is denied, the school or department may request reasons for the denial in writing.

If the request is approved, the school or department must submit to the ~~D~~director of ~~M~~media and ~~T~~technology ~~S~~services, within two weeks of developing the site, the name of the person(s) who will manage the site and the login information for the site. When a presence is established, the sponsoring school or department is responsible for keeping the site current and monitoring the content of the site.

Sites may be linked from the official district website. All sites must comply with web ~~publishing guidelines~~ found in ~~Policy 634 (Electronic Technologies Acceptable Use) and~~ record retention requirements under Policy 719 (Records Retention.).

Revised: 9/24/12
Reviewed: 4/20/20
Revised: 8/8/22

Appendix VI to ~~Policy 634~~ Policy 524

GUIDELINES FOR DISTRICT SOCIAL MEDIA PAGES

The school district's social media presence creates an accessible communications outlet, providing district news, facilitating district-related discussion by the community, and guiding viewers to departmental websites at www.edinaschools.org. These guidelines are used in conjunction with Policy ~~634~~ 524 (Electronic Technologies Acceptable Use) and all other district policies.

Establishment of Page

1. The district will include on its social media page, in a prominent location, a link to the Edina Public Schools' website, as well as contact information for the district.

2. The district will include language regarding limitation on comments and posts by its users:

   Any comments/posts viewed as inappropriate or offensive are subject to removal without notice. These comments/posts include, but are not limited to, commercial solicitations; factually erroneous/libelous information; vulgarity or obscenity; personal attacks of any kind; political support or opposition to any candidate or political measure; offensive comments that target or disparage any group/person; violations of district policy; or discussions not related to the district.

3. The district will include language regarding compliance with data practices and records retentions under Minnesota law:

   Social ~~M~~media pages are intended to serve as a mechanism for communication between the public and ~~Edina Public Schools~~ the district. Any comments submitted to pages, and its list of ~~fans~~ followers or subscribers, are public records subject to disclosure and retention pursuant to Minnesota law. Public disclosure requests must be directed to ~~Edina Public Schools~~ the district.

4. The communications department will be responsible for monitoring the district social media pages, including content and comments, to ensure compliance with guidelines for use as posted on the social media pages.

Postings

The district will provide balance in topics shared on its social media pages. District posts will highlight information relevant to and of interest to the community as a whole. Postings may also include prompts or questions relevant to the work and mission of the district that are intended to engage the community in the work of the district. Suggestions for posts should be submitted to the ~~D~~director of ~~M~~marketing and ~~C~~communications.

Revised: 12/10/12
Modified: 11/13/17
Reviewed: 4/20/20
Revised: 8/8/22

Appendix VII to ~~Policy 634~~ Policy 524

Personal Device Access

Users of personal devices connecting to Edina-Open must abide by Edina Public Schools' Policy 524 (Electronic Technologies Acceptable Use)~~Policy (Board Policy 634)~~. Though guests may use their personal device and expect some aspects of privacy, use of ~~our~~ the school district's network and systems have the following expectations:

1. Use at your own risk. Use of the ~~Edina Public Schools~~ district network is at the device owner's discretion and therefore ~~Edina Public Schools~~ the district is not responsible for any loss, damage or adverse effects that may occur to a device while on ~~our~~ the district network.

2. Devices need to be registered. All non-district devices connected to the ~~Edina Public Schools~~ district network need to be registered. In the event of a security incident, personal devices may be disconnected without notice. No support for remediation of security incidents (e.g., malware) will be available, and devices will remain disabled from ~~our~~ the district network until fixed.

3. The ~~Edina Public Schools~~ district network is monitored. For security purposes and ~~following~~ pursuant to federal law, the district has implemented monitoring of ~~our~~ the district network. Personal devices connected to ~~our~~ the district network will also be monitored for access, times, network content, and known security vulnerabilities. This information may be recorded~~,~~ and is subject to audit.

4. The ~~Edina Public Schools~~ district network~~s are~~ is filtered. Known inappropriate and/or malicious sites, and many non-instructional sites, are blocked. Use of the district network and systems requires that owners of personal devices adhere to legal and ethical conduct, and refrain from attempting to access blocked content.

5. No ~~E~~expectation of privacy. Access to the contents of personal devices is governed by local and federal laws. However, while accessing the ~~Edina Public Schools~~ district network, systems, and buildings, there is not a right to privacy of any content, and as such, may be ~~monitored~~ accessed for inappropriate or illegal activities.

6. ~~Edina Public Schools~~ The district reserves the right to maintain records of usage. ~~Edina Public Schools~~ The district may immediately terminate the privilege to use the ~~Edina Public Schools~~ district network should it become aware that the network is being used for inappropriate or illegal activities. The district reserves the right to take appropriate action in the event inappropriate or illegal activities are discovered on ~~our~~ the district systems or network.