524 INTERNET AND ELECTRONIC RESOURCES ACCEPTABLE USE AND SAFETY POLICY

I. PURPOSE

The purpose of this policy is to define acceptable use of the school district technology system, provide guidelines for use of personal devices within the district and set forth policies establishing acceptable and safe use of the Internet and cloud-based tools, including electronic communications.

II. GENERAL STATEMENT OF POLICY

In making decisions regarding student and employee access to the school district technology system, which includes, but is not limited to, electronic resources, cloud-based tools, access to the Internet, and electronic communications (referred to throughout this policy as simply "district technology system"), the school district considers its own stated educational mission, goals, and objectives. Electronic information research skills are now fundamental to preparation of citizens and future employees. Access to the district technology system and to the Internet enables students and employees to explore thousands of libraries, databases, bulletin boards, and other resources while exchanging messages with people around the world. The school district expects that faculty will blend thoughtful use of the district technology system and the Internet throughout the curriculum and will provide guidance and instruction to students in their use. The school district views parents/guardians as partners in the oversight of students in regard to their acceptable use of technology, each with their own responsibilities as described in this policy.

III. DEFINITIONS

A. *Electronic Resources* include but are not limited to network systems and components, computers and peripherals, printers, telephones, network systems and components, and the applications they support and/or access. These items may or may not be owned by the school district.

B. *Cloud-based Tools* refers to websites and applications within the World Wide Web that focus on user collaboration, sharing of user-generated content, and social networking rather than simply displaying static content.

IV. LIMITED EDUCATIONAL PURPOSE

The school district provides students and employees (including volunteers and contractors performing services for the school district) access to the district technology system. The

purpose of the district technology system is more specific than providing students and employees with general access to the Internet. The district technology 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 technology system to further educational and personal goals consistent with the mission of the school district and school policies and handbooks. Uses which might be acceptable on a user's private personal account on another system may not be acceptable on this limited-purpose network.

See Addendum I, Student Online Code of Ethics

V. USE OF SYSTEM IS A PRIVILEGE

The use of the district technology 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 school 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 school district policies, including suspension, expulsion, exclusion, or termination of employment; or civil or criminal liability under other applicable laws.

Use of personal (employee or student owned) electronic resources, (including personal cell phones or other personal devices) during time an employee is being paid to work, and/or while employees and students are on district property, is subject to all district policies and handbooks, as applicable, in addition to any state and federal laws related to Internet use, including copyright laws.

All work created by school district employees using the district technology system, resources or on school district time is the property of the school district.

See Addendum II, Guidelines for Employee's Personal Use of Social Networking
See Addendum III, Guidelines for Classroom Use of Social Media Tools

VI. UNACCEPTABLE USES

A. The following uses of the district technology system and Internet resources or accounts on or off district property and/or personal electronic resources while at work or on district property and/or the district technology system are considered unacceptable:

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

a. pornographic, obscene, or sexually explicit material or other visual depictions that are harmful to minors;

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

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

d. information or materials that could cause damage or danger of disruption to the educational process;

e. materials that use language or images that advocate violence or discrimination toward other people (hate literature) or that may constitute harassment or discrimination.

2. Users will not use the district technology 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.

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

4. Users will not use the district technology 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 or by any other means, will not tamper with, modify, or change the district technology system software, hardware, or wiring or take any action to violate the school district's security system, and will not use the district technology system in such a way as to disrupt the use of the system by other users.

5. Users will not use the district technology system to gain unauthorized access to information resources or to access another person's materials, information, or files without the implied or direct permission of that person.

6. Users shall not use the district technology system to record, photograph or video students or school employees on school property, on a school bus or at school-sponsored activities without their knowledge and consent, except for activities considered to be in the public arena (e.g. sporting events, public meetings, academic competitions or public performances). School social events, activities sponsored by student clubs, team building retreats, and activities that take place during the school day are not considered to be in the public arena.

7. Users will not use the district technology system to post 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 school district webpages, social media sites 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).

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 school district as directory information and verification is made that the school 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; or

(2) such information is not classified by the school 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.

(3) such information is discoverable or obtained from a media source or public website.

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 technology system to post personal information about a user or another individual on social networks, including, but not limited to, social networks such as "Facebook", "Twitter", "Instagram", "Snapchat", and "Reddit", and similar websites and applications.

8. Users must keep all account information and passwords on file with the designated school district official. Users will not attempt to gain unauthorized access to the district technology system or any other system through the district technology 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 technology system may not be encrypted without the permission of appropriate school authorities.

9. Users will not use the district technology 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.

10. Users will not use the district technology system for conducting non-district business, including, but not limited to, unauthorized commercial purposes, financial gain unrelated to the mission of the school district, offering or providing goods or services, product advertisement or purchasing goods or services for personal use without authorization from the appropriate school district official.

11. Users will not use the district technology system to engage in bullying or cyberbullying in violation of the school district's Bullying Prohibition Policy (District 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.

12. Users may not add or remove any software nor modify the equipment, software configuration, or environment. Users will not install any personal equipment or software on any district-owned system.

B. A student or employee engaging in the foregoing unacceptable uses of the Internet when off school district premises also may be in violation of this policy as well as other school district policies and handbooks. Examples of such violations include, but are not limited to, situations where the district technology system is compromised or if a school district employee or student is negatively impacted. If the school district receives a report of an unacceptable use originating from a non-school computer or resource, the school 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 school district computer system and the Internet and discipline under other appropriate school district policies, including suspension, expulsion, exclusion, or termination of employment.

See addendum IV, School-Issued Devices

C. If a user inadvertently accesses unacceptable materials or an unacceptable Internet site, the user shall immediately disclose the inadvertent access to an appropriate school district official. In the case of a school district employee, the immediate disclosure shall 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. In certain rare instances, a user also may access otherwise unacceptable materials if necessary to complete an assignment and if done with the prior approval of and with appropriate guidance from the appropriate teacher or, in the case of a school district employee, the building administrator.

VII. FILTER

School districts which receive certain federal funding, such as e-rate discounts, for purposes of Internet access and connection services and/or receive funds to purchase Internet accessible computers are subject to the federal Children's Internet Protection Act ("Act"). This Act

requires school districts to adopt an Internet safety policy, which contains the provisions set forth below. Also, the Act requires such school districts to provide reasonable notice and hold at least one public hearing or meeting to address the proposed Internet safety policy prior to its implementation. School districts that do not seek such federal financial assistance need not adopt the alternative language set forth below nor meet the requirements with respect to a public meeting to review the policy. The following alternative language for school districts that seek such federal financial assistance satisfies both state and federal law requirements.

A. With respect to any of its computers with Internet access, the school district will monitor 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. An administrator, supervisor, or other person authorized by the Superintendent may disable the technology protection measure, during use by an adult, to enable access for bona fide research or other lawful purposes.

D. The school district will educate students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyber-bullying awareness and response.

E. Software filtering technology will be narrowly tailored and will not discriminate based upon viewpoint.

VIII. CONSISTENCY WITH OTHER SCHOOL POLICIES

Use of the district technology system and use of the Internet shall be consistent with school district policies, handbooks and the mission of the school district.

IX. LIMITED EXPECTATION OF PRIVACY

A. By authorizing use of the district technology system, the school 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 technology system.

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

C. An individual investigation or search will be conducted if school authorities have a reasonable suspicion that the search will uncover a violation of law or school district policy. This may include a search of an employee's or student's personal cell phone or other portable electronic devices, if there is reason to believe the employee or student used the device during working hours and/or on school property.

D. Parents/guardians, in accordance with district policy and state and federal laws, have the right at any time to investigate or review the contents of their child's files and e-mail files. Parents/guardians have the right to request the termination of their child's individual account at any time.

E. School district employees should be aware that the school district retains the right at any time to investigate or review the contents of their files and e-mail files. In addition, school district employees should be aware that data and other materials in files maintained on the district technology 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 school district policies conducted through the district technology system.

X. INTERNET AND ELECTRONIC RESOURCES USE AGREEMENT

A. The proper use of the Internet and district technology system and the educational value to be gained from proper use of the Internet and district technology system, 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 designated professional staff before a student may use a school account or resource to access the Internet.

C. The Internet and Electronic Resources Use Agreement form and the addendum for students must be read and signed by a parent or guardian in grades K, 5 and 9 or when the student is first enrolled in the district. The Internet and Electronic Resources Use Agreement form and the addendum for students must be read and signed by the user student in grades 5 and 9 or when a student in those grades is first enrolled in the district. The agreement is effective throughout the child's education at their school. All students (K-12) will review and all parents and guardians will receive a notice regarding the school district policies and addenda relating to safety and acceptable use

of the district's technology system annually. The Internet and Electronic Resources Use Agreement form and addendums for employees must be signed by the employee upon hire. The form must then be filed physically or electronically at the school or school district office.

XI. LIMITATION ON SCHOOL DISTRICT LIABILITY

Use of the district technology system is at the user's own risk. The system is provided on an "as is, as available" basis. The school 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, tapes, hard drives, or servers, or for delays or changes in or interruptions of service or mis-deliveries or non-deliveries of information or materials, regardless of the cause. The school district is not responsible for the accuracy or quality of any advice or information obtained through or stored on the district technology system. The school district will not be responsible for financial obligations arising through unauthorized use of the district technology system or the Internet. The school district assumes no responsibility for theft, loss, or damage of a personal electronic device brought to school/work and will not assume responsibility for investigating loss or theft of such items.

XII. USER NOTIFICATION

A. All users shall be notified of the school district policies relating to use of the district technology system and the Internet.

B. This notification shall include the following:

1. Notification that use of the district technology system and the Internet is subject to compliance with school district policies.

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

a. Information stored on school district cloud-based applications, hard drives, servers, CD, DVD, memory stick or similar devices, or any other storage device.

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

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

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

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

4. Notification that, even though the school 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 Policy 406, Public and Private Personnel Data, and Policy 515, Protection and Privacy of Pupil Records.

7. Notification that, should the user violate the school 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 and cloud-based tool 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 district technology system and of the Internet from home or a remote location.

B. Parents/guardians will be notified that their students will be using school district technology resources/accounts to access the Internet and cloud-based tools, that teachers and other district staff will be communicating with students using electronic resources and cloud-based tools, and that the school 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 notification that the parents/guardians have the option to request alternative educational activities not requiring Internet access and the material to exercise this option.

4. A statement that the Internet and Electronic Resources Use Agreement must be signed by the user and a parent or guardian, prior to use by the student.

5. A statement that the school district's acceptable use policy is available for parent/guardian review.

See Addendum V, Notification Regarding Technology Providers

XIV. 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 school has an individualized family service plan, an individualized education program, or a 504 plan in effect.

XV. IMPLEMENTATION; POLICY REVIEW

A. The school district administration may develop appropriate user notification forms, guidelines, and procedures necessary to implement this policy.

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

C. The school 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, District Administration shall conduct an annual review of this policy.

Legal References:
Minn. Stat. Ch. 13 (Minnesota Government Data Practices Act)
Minn. Stat. § 13.32 (Educational Data)
Minn. Stat. § 121A.031 (School Student Bullying Policy)
Minn. Stat. § 124D.166 (Limit on Screen Time for Children in Preschool and Kindergarten)
Minn. Stat. § 125B.15 (Internet Access for Students)
Minn. Stat. § 125B.26 (Telecommunications/Internet Access Equity 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)
47 U.S.C. § 254 (Children's Internet Protection Act of 2000 (CIPA))
47 C.F.R. § 54.520 (FCC rules implementing CIPA)
Mahanoy Area Sch. Dist. 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. Amer. Library Assoc., 539 U.S. 1942003)
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: School District Policy 403 (Discipline, Suspension, and Dismissal of School District Employees)
School District Policy 406 (Public and Private Personnel Data)
School District Policy 505 (Distribution of Nonschool-Sponsored Materials on School Premises by Students and Employees)
School District Policy 506 (Student Discipline)
School District Policy 514 (Bullying Prohibition Policy)
School District Policy 515 (Protection and Privacy of Pupil Records)
School District Policy 519 (Interviews of Students by Outside Agencies)
School District Policy 521 (Student Disability Nondiscrimination)
School District Policy 522 (Student Sex Nondiscrimination)
School District Policy 603 (Curriculum Development)
School District Policy 604 (Instructional Curriculum)
School District Policy 806 (Crisis Management Policy)
School District Policy 904 (Distribution of Materials on School District Property by Nonschool Persons)

POLICY ADOPTED: October 16, 2006
POLICY REVIEWED/REVISED: December 14, 2009; June 17, 2013; March 21, 2016; December 17, 2018; November 18, 2019; November 16, 2020; August 2, 2021; April 17, 2023; September 18, 2023
Monitoring Method: Administrative Review
Monitoring Frequency: Every year

ADDENDUM I - STUDENT ONLINE CODE OF ETHICS

In the West St. Paul-Mendota Heights-Eagan Area Schools, it is important to use information and technology in safe, legal, and responsible ways. 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 cloud-based tools including, but not limited to, blogs, wikis, podcasts, Google applications, Canvas and SeeSaw for student assignments are required to keep personal information out of their postings.

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

3. Students must not log in to the network as another classmate.

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

5. Assignments on cloud-based 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 and acceptable use of technology.

6. Student blogs 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 board policy.

7. Students must not use the Internet to harass, discriminate, bully or threaten the safety of others. If students receive a comment on a blog or other cloud-based tool used in school that makes them feel uncomfortable or is not respectful, they must report this to a teacher, and must not respond to the comment.

8. Students accessing cloud-based tools from home or school, using the district technology system, must not download or install any software without permission, and not click on ads or competitions.

9. Students should be honest, fair and courageous 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 must 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.

11. Students are accountable to their readers, listeners and viewers and to each other. Students should admit their mistakes and correct them promptly, while also exposing the unethical information and practices of others.

12. Students shall not record, photograph or video other students or school employees on school property, on a school bus or at school-sponsored activities without their knowledge and consent, except for activities considered to be in the public arena (e.g. sporting events, public meetings, academic competitions or public performances). School social events, activities sponsored by student clubs, team building retreats, and activities that take place during the school day are not considered to be in the public arena.

13. School board policies concerning acceptable use of electronic technology include the use of these cloud-based tools for school activities (Policy 524 – Internet and Electronic Resources Acceptable Use).

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

ADDENDUM II - GUIDELINES FOR EMPLOYEE'S PERSONAL USE OF SOCIAL NETWORKING

The decision to use online social networking (including, but not limited to, sites such as Facebook and online chat rooms, blogs, wikis, podcasts, discussion boards, etc.) 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 the district technology system; 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. In addition, if an employee chooses to engage in social networking during working hours, this activity may be subject to review by the school district. These guidelines are for employees engaging in social networking for personal use.

1. When using your personal social networking sites, do not fraternize 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.

6. Respect your coworkers and students and remain professional. Do not discuss students, their families or coworkers.

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

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

9. The school district recognizes that student groups or members of the public may create social media representing students or groups within the school district. When employees, including coaches/advisors, choose to join or engage with these school district-related social networking groups or forums, they do so as an employee of the school district. Employees have responsibility for maintaining appropriate employee-student relationships at all times and have responsibility for addressing inappropriate behavior or activity on these networks. This includes acting to protect the safety of minors online.

10. When engaging in non-school district related social networking groups or forums, the public may consider your personal statements as being made in your capacity as a district employee. Employees may want to include "this posting is my own and does not represent the view of West St. Paul-Mendota Heights-Eagan Area Schools (School District 197)." An employee in a leadership role in the school district, by virtue of their position, must consider whether personal thoughts they publish~~es~~ will be attributed to the school district.

11. Social media identifications, login identifications, and user names must not contain the school district or school's name or logo without prior written permission from (1) the director of technology and (2) the director of communications.

ADDENDUM III - GUIDELINES FOR CLASSROOM USE OF SOCIAL MEDIA TOOLS

The school district provides teachers with webpages and password-protected, online social media tools that can be used for communication and instruction. Teachers may also elect to use other social media tools for the purpose of instruction in accordance with Policy 524 – Internet and Electronic Resources Acceptable Use and its appendices.

A. District Online Social Media Tools

1. Content and use must adhere to school 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 West St. Paul-Mendota Heights-Eagan Area Schools (School District 197).

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

B. Non-district Social Media Tools

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

2. Approval must be received from (1) the director of communications and (2) the director of technology prior to creation of the page. The request must contain the following:

   a. Sponsoring school or department;
   b. Proposed social media site or other location;
   c. Purpose of site, which cannot be served by the current district website;
   d. Plan on how to comply with district policies and mandated reporting and record retention requirements;
   e. Description and primary use of site;
   f. Plan for monitoring site, addressing policy violations, and ensuring current content, notifying parents/guardians of their child's participation in the site; and
   g. Name of the person(s) who will manage the site and the login information for the site.

   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.

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

4. Content and use must not violate the "terms of service" for the social media tool.

5. 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 West St. Paul-Mendota Heights-Eagan Area Schools (School District 197).

6. The teacher must not disclose information on any online social media site that is protected by data privacy laws, or in violation of copyright.

7. The platform must not use official school district or school logos without the permission of (1) the director of communications or superintendent's designee and (2) the director of technology.

ADDENDUM IV - SCHOOL-ISSUED DEVICES

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

B. Except as provided in paragraph C, the school district or a technology provider must 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.

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

1. the activity is limited to a noncommercial educational purpose for instruction, technical support, or exam-proctoring by school district employees, student teachers, staff contracted by the school 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 school 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, including but not limited to Minnesota Statutes section 121A.031; or

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

D. If the school district or a technology provider interacts with a school-issued device as provided in paragraph C, clause 4, it must, within 72 hours of the access, notify the student to whom the school-issued device was issued or that student's parent/guardian and provide a written description of the interaction, including which features of the device were accessed and a description of the threat. This notice is not required at any time when the notice itself would pose an imminent threat to life or safety, but must instead be given within 72 hours after that imminent threat has ceased.

ADDENDUM V - NOTIFICATION REGARDING TECHNOLOGY PROVIDERS

A. "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.

B. "Parent/Guardian" means a parent/guardian of a student and includes a natural parent, a guardian, or an individual acting as a parent/guardian in the absence of a parent or a guardian.

C. Within 30 days of the start of each school year, the school district must 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 must:

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.

D. The school district must provide parents/guardians and students with an opportunity to inspect a complete copy of any contract with a technology provider.

E. A contract between a technology provider and the school district must include requirements to ensure appropriate security safeguards for educational data. The contract must 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.

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

POLICY 524 - INTERNET AND ELECTRONIC RESOURCES USE AGREEMENT STUDENT / PARENT OR GUARDIAN

STUDENT

I have read and do understand the school district policies and addenda relating to safety and acceptable use of the district technology system, which includes electronic resources, cloud-based tools, electronic communications and Internet resources or accounts on or off school district property and/or personal electronic resources while on district property and/or the district technology system and agree to abide by them. I understand that the school district may need to search any school district-owned technology that has been provided to me to determine if I have committed a violation of school district rules, and give my consent for the school district to conduct such a search. I further understand that should I commit any violation of these policies and addenda, my access privileges may be revoked, school disciplinary action may be taken, and/or appropriate legal action may be taken.

Signature required if student is new to the school district or in grades 5 or 9.

User's Full Name (please print): _____

User Signature: _____

Student ID Number: _____ Date: _____

PARENT OR GUARDIAN

As the parent or guardian of this student, I have read and discussed with my child the school district policies and addenda relating to safety and acceptable use of the district technology computer system, which includes electronic resources, cloud-based tools, electronic communications and Internet resources or accounts on or off school district property and/or personal electronic resources while on district property and/or the district technology system. I understand that this access is designed for educational purposes. The school district has taken precautions to eliminate controversial material.
However, I also recognize it is impossible for the school district to restrict access to all controversial materials and I will not hold the school district or its employees or agents responsible for materials acquired on the Internet. Further, I accept full responsibility for supervision if and when my child's use is not in a school setting. I hereby give permission to issue an account for my child and certify that the information contained on this form is correct.

Signature required if student is new to the school district or in grades K, 5 or 9.

Parent or Guardian's Name (please print): _____

Parent or Guardian's Signature: _____

POLICY 524 - INTERNET AND ELECTRONIC RESOURCES USE AGREEMENT EMPLOYEE

SCHOOL DISTRICT EMPLOYEE

I have read and do understand the school district policies relating to safety and acceptable use of the district technology system, which includes electronic resources, cloud-based tools, electronic communications and Internet resources or accounts on or off school district property and/or personal electronic resources while on school district property and/or the district technology system and agree to abide by them. I further understand that should I commit any violation, my access privileges may be revoked, school disciplinary action may be taken, and/or appropriate legal action may be taken. I also understand that the school district may need to search any school district-owned technology that has been provided to me and any personal electronic devices I have used while acting in the scope of my employment to determine if I have committed a violation of school district policy, and give my consent for the school district to conduct such a search.

User's Full Name (please print): _____

User Signature: _____

Date: _____