524 INTERNET ACCEPTABLE USE AND SAFETY POLICY

I. Purpose

This policy sets forth policies, parameters and guidelines for access to the district's electronic technologies, use of personal electronic devices within the district, electronic communications, use of the district's network, Internet, and social networking tools.

II. General Statement of Policy

In making decisions regarding employee and student access to the district's computer network, use of electronic technologies and Internet, the district considers its own educational mission, goals and strategic direction. Access to the district's computer network and Internet enables students and employees to explore libraries, databases, web pages, other online resources, and exchange messages with people around the world. The district expects its instructional staff to blend safe and thoughtful use of the district's computer network, educational technologies and the Internet throughout the curriculum, providing guidance to students.

III. Educational Purposes

The district purpose in offering access to the district's electronic technologies or use of personal technology devices for students and employees is more specific than providing them with general access. Use of the district's electronic technologies is for educational purposes. Students and employees are expected to use electronic technologies to further the district's educational mission, goals and strategic direction. Students and employees are expected to use the district's electronic technologies to support classroom activities, educational research or professional enrichment.

Use of the district's electronic technologies is a privilege, not a right. Misuse of the district's electronic technologies may lead to discipline of the offending employee or student. The district's network, an educational technology, is a limited forum; the district may restrict speech for educational reasons.

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 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 acceptable laws.

V. Guidelines in Use of Electronic Technologies

A. 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.
B. The district reserves the right to monitor, read or copy any item on or using the district's electronic technologies, including its network.
C. Students and employees will not vandalize damage or disable any electronic technology or system used by the district.
D. By authorizing use of the district system, the district does not relinquish control over materials on the system or contained in files on the system.
E. Users should not expect privacy in the contents of personal files on the district system.
F. Routine maintenance and monitoring of electronic technologies, including the district network, may lead to a discovery that a user has violated this policy, another school district policy or the law.

VI. Unacceptable Uses of Electronic Technologies and District Network

The following uses of district electronic technologies while either on or off district property and/or personal electronic technologies while on district property and district network ("electronic technologies") are considered unacceptable:

A. Users will not use electronic technologies to create, access, review, upload, download, complete, store, print, post, receive, transmit or distribute:
    1. Pornographic, obscene or sexually explicit material or other visual depictions;
    2. Obscene, abusive, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful or sexually explicit language;
    3. Materials that use language or images that are inappropriate in the education setting or disruptive to the educational process;

4. Materials that use language or images that advocate violence or discrimination toward other people or that may constitute harassment, discrimination or threatens the safety of others;
5. Orders for shopping online during time designated as work time by the district; and
6. Storage of personal photos, videos, music or files not related to educational purposes for any length of time.

B. Users will not use electronic technologies 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.
C. Users will not use electronic technologies to engage in any illegal act or violate any local, state or federal laws.
D. Users will not use electronic technologies for political campaigning.
E. Users will not use electronic technologies to vandalize, damage or disable the property of another person or organization. Users 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. Users will not tamper with, modify or change the district system software, hardware or wiring or take any action to violate the district's security system. Users will not use the district's electronic technologies in such a way as to disrupt the use of the system by other users.
F. Users will not use electronic technologies 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.
G. Users must not deliberately or knowingly delete a student or employee file.
H. Users will not use electronic technologies to post information in public access areas regarding private or confidential information about another person. Private or confidential information is defined by board policy, state law, and federal law.
    1. This paragraph does not prohibit the posting of employee contact information on district web pages.
    2. This paragraph does not prohibit communications between employees and other individuals when such communications are made for legitimate education reasons or personnel-related purposes (i.e. communications with parents or other staff members related to students).
    3. This paragraph specifically prohibits the use of electronic technologies to post private or confidential information about another individual, employee or student, on social media.
I. Users will not repost or resend a message that was sent to the user privately without the permission of the person who sent the message.
J. Users will not attempt to gain unauthorized access to the district's electronic technologies or any other system through electronic technologies, 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. Users must keep all account information and passwords private.
K. Messages and records on the district's electronic technologies may not be encrypted without the permission of director of media and technology services.
L. Users will not use electronic technologies to violate copyright laws or usage licensing agreements:
    1. Users will not use another person's property without the person's prior approval or proper citation;
    2. Users will not download, copy or exchange pirated software including freeware and shareware; and
    3. Users will not plagiarize works found on the Internet or other information resources.
M. Users will not use electronic technologies for unauthorized commercial purposes or financial gain unrelated to the district's mission. Users will not use electronic technologies to offer or provide goods or services or for product placement.

VII. User Notification

Users will be notified of the district policies relating to Internet use. This notification must include the following:

A. Notification that Internet use is subject to compliance with district policies.
B. Disclaimers limiting the district's liability relative to:
    1. Information stored on district disks, drives or servers.
    2. Information retrieved through district computers, networks or online resources.
    3. Personal property used to access district computers, networks or online resources.
    4. Unauthorized financial obligations resulting from use of district resources or accounts to access the Internet.
C. A description of the privacy rights and limitations of district sponsored or managed Internet accounts.
D. Notification that the collection, creation, reception, maintenance and dissemination of data via the Internet, including electronic communications, is governed.
E. Notification that should the user violate the district's acceptable use policy, the user's access privileges may be revoked, academic sanctions may result, school disciplinary action may be taken, and/or appropriate legal action may be taken.
F. Notification that all provisions of the acceptable use policy are subordinate to local, state and federal laws.
G. Family Notification
    1. Notification that the district uses technical means to limit student Internet access however, the limits do not provide a foolproof means for enforcing the provisions of this acceptable use policy.
    2. 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 or the student's parents.

VIII. Students

A. Internet Use Agreement
    1. The proper use of the Internet and educational technologies and the educational value to be gained from proper usage is the joint responsibility of students, parents and employees of the district.
    2. This policy requires the permission of and supervision by the school's designated professional staff before a student may use a district account or educational technologies to access the Internet.
    3. The Internet Use Agreement form (see Appendix VI) for students must be read and signed by the student and the parent or guardian. The agreement must be signed in order to be granted access to the Internet via the district network. This policy requires that the signed, up-to-date form be retained electronically or physically.
    4. A physical or electronic signature is required when the student begins in the district, in Kindergarten, in 5th grade and in 9th grade.
    5. Students have access to Internet resources while on district property.
    6. Students using social networking tools and curriculum content management software for a teacher's assignment are required to keep personal information as stated above out of their postings (see SectionV.H).
    7. Students using educational technologies for social networking are limited to educational purposes and must follow the Online Code of Ethics (Appendix I).

B. Parents' Responsibility; Notification of Student Internet Use. Outside of school, parents bear responsibility for the same guidance of Internet use as they exercise with other technology information sources. Parents are responsible for monitoring their student's use of the district system and district educational technologies, even if the student is accessing the district system from home or a remote location.

IX. Guest Access and Internet Use

A. Guest access to the 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.

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.

X. Employees

A. Use of Email.

The 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 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.
5. All emails to a student's parents or guardians about a student must adhere to the following precautions:
    a. Do not use email to communicate about confidential student information unless the parent or guardian has requested the communication.
    b. Do not put information in an email that you would not put on district letterhead.
    c. Emails containing student information should be sent to the parent or guardian's personal email address unless requested otherwise.
    d. A phone call is the means for sharing confidential student information. Do not leave voice mail messages containing confidential information.
6. Employees will not provide access to their email accounts to nonemployees.
7. All emails should include the employee's name and telephone number at the bottom of the email.
8. It is recommended that electronic mail contain a confidentiality notice, similar to the following:
   If the information in this email relates to an individual or student, it may be private data under state or federal privacy laws. This individual private data should not be reviewed, distributed or copied by any person other than the intended recipient(s), unless otherwise permitted under law. If you are not the intended recipient, any further review, dissemination, distribution, or copying of this electronic communication or any attachment is strictly prohibited. If you have received an electronic communication in error, you should immediately return it to the sender and delete it from your system.
9. Employees will report inappropriate emails to the media specialist, the employee's supervisor or the director of media and technology.

10. Emails having content governed by the district's record retention schedule must be kept in accordance with the retention schedule.

B. Use of Electronic Technologies
   1. Electronic technologies are provided primarily for work-related, educational purposes.
   2. Inappropriate use of electronic technologies includes, but is not limited to:
      a. Posting, viewing, downloading or otherwise receiving or transmitting offensive, defamatory, pornographic or sexually explicit materials;
      b. Posting, viewing, downloading or otherwise receiving or transmitting materials that use language or images that advocate violence or discrimination toward other persons;
      c. Posting, viewing, downloading or otherwise receiving or transmitting material that may constitute harassment or discrimination contrary to district policy and state and federal law;
      d. Engaging in computer hacking or other related activities;
      e. Attempting to, actually disabling or compromising the security of information contained on the district network or any computer; and
      f. Engaging in any illegal act in violation of any local, state or federal laws.
   3. Employees may participate in public Internet discussion groups using the electronic technologies, but only to the extent that the participation:
      a. Is work-related;
      b. Does not reflect adversely on the district;
      c. Is consistent with district policy; and
      d. Does not express any position that is, or may be interpreted as, inconsistent with the district's mission, goal or strategic plan.
   4. Employees may not use the district network or electronic technologies to post unauthorized or inappropriate personal information about another individual on social networks.
   5. Employees will observe all copyright laws. Information posted, viewed or downloaded from the Internet may be protected by copyright.
   6. All files downloaded from the Internet must be checked for possible computer viruses. The district authorized virus checking software installed on each district computer will ordinarily perform this check automatically; however, employees should contact the district's director of media and technology services before downloading any materials for which the employee has questions.

C. Employee Responsibilities
   1. Employees who are transferring positions or leaving positions must leave all work-related files and electronic technologies, including form letters, handbooks, databases, procedures, and manuals, regardless of authorship, for their replacements.
   2. Individual passwords for computers are confidential and must not be shared.
      a. If an employee's password is learned by another employee, the password should be changed immediately.
      b. An employee is responsible for all activity performed using the employee's password.
      c. No employee should attempt to gain access to another employee's documents with prior express authorization.
      d. An active terminal with access to private data must not be left unattended and must be protected by password protected screen savers.
   3. Employees are expected to use technology necessary to perform the duties of their position.
   4. Employees who fail to adhere to district policy are subject to disciplinary action in accordance with their collective bargaining agreement or contract. Disciplinary action may include suspension or withdrawal of Internet or email access, payment for damages or repair, termination and/or referral to civil or criminal authorities for prosecution.

XI. District Web Presence

The district website was established to provide a learning experience for employees and students and to provide a venue for communications with parents and the community.

A. District Website
   1. The district will establish and maintain a website. The website will include information regarding the district, its schools, district curriculum, extracurricular activities and community education.
   2. The district webmaster will be responsible for maintaining the district website and monitoring district web activity.
   3. All website content will support and promote the district's mission, goals and strategic direction.
   4. The district's website will provide parents with a web portal to classroom related calendars, grades, attendance, assignments and resources.

B. School Website
   1. Each school will establish and maintain a website. The website will include information regarding the school, its employees, and activities.
   2. The principal will appoint staff, who will be responsible for maintaining the school's website.
   3. All website content will support and promote the district's mission, goals and strategic direction.

4. Each school's website will provide parents with a web portal to classroom related calendars, grades, attendance, assignments and resources.

C. Classroom and Teacher Web Content
   1. The district encourages all teachers to establish a web page that supports their classroom instruction.
   2. If a teacher establishes a web page, he or she is responsible for maintaining the web page.
   3. All classroom and teacher web pages must be linked to a school website.

D. Student Web Content
   1. Students may create web pages as part of classroom activities with teacher supervision.
   2. Student web pages must follow the Online Code of Ethics, Appendix I and include the following notice: "This is a student-produced web page. Opinions expressed on this page are not attributable to the district."
   3. The classroom teacher will monitor all student-produced web content and remove inappropriate material.
   4. A classroom teacher or advisor will review student-produced web pages to determine if the contents should be removed at the conclusion of the course grading period, or activity.

E. Department and non-instructional Web Content
   1. Departments and non-instructional programs may also create web content, including web pages to support their departments or programs.
   2. The establishment of web pages must be approved by the program administrator.
   3. Once established, the individual departments or programs must appoint an employee(s) who will maintain the web page.

F. District Activity Web Content
   1. With the approval of the building principal, a school board-approved district activity may establish a web page.
   2. All web page content will support the activity and the district's mission, goals and strategic direction.
   3. The building principal and his/her designee will oversee the content of these web pages.
   4. School board-approved district activities' web pages must include the following notice: "This is an organization-produced web page. Opinions expressed on this page are not attributable to the district."

XII. Records Management and Archiving

All technological data is data under the Minnesota Government Data Practices Act, the Family Educational Rights and Privacy Act, Records Retention Schedule, and school board policy.

XIII. Consistency with other School Policies

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

XIV. Limited Expectation of Privacy

A. By authorizing use of the school district 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 school 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 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.

D. Parents have the right at any time to investigate or review the contents of their child's files and e-mail files. Parents 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 school 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 school district policies conducted through the school district system.

XI. 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, 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 Use Agreement form for students must be read and signed by the user, the parent or guardian, and the supervising teacher. The Internet Use Agreement form for employees must be signed by the employee. The form must then be filed at the school office. As supervising teachers change, the agreement signed by the new teacher shall be attached to the original agreement.

XVI. Filter

A. With respect to any of its computers with Internet access, and personal devices accessing the district network, the district will follow the guidelines provided by the Children's Internet Protection Act, and will monitor the online activities of users and employ technology protection measures during any use of such computers by users. 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.

XVII. Liability

Use of the district's educational technologies 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. The district is not responsible for the accuracy or quality of any advice or information obtained through or stored on the school district system, nor is it responsible for damages or injuries from improper communications or damage to property used to access school computers and online resources. The district will not be responsible for financial obligations arising through unauthorized use of the district's educational technologies or the Internet.

By this language, as a public governmental entity, the indemnity clause of Facebook's Statement of Rights and Responsibilities is nullified.

XVIII. Parents' Responsibility; Notification of Student Internet Use

A. Outside of school, parents 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 are responsible for monitoring their student's use of the school district system and of the Internet if the student is accessing the school district system from home or a remote location.

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

C. This notification includes:
   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 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 Use Agreement must be signed by the user, the parent or guardian, and the supervising teacher prior to use by the student.
   5. A statement that the school district's acceptable use policy is available for parental review.

XIII. 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" means a parent of a student and includes a natural parent, a guardian, or an individual acting as a parent 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 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 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 and students 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.

XIV. 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 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.

XV. 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.

XIX. Implementation; Policy Review

A. The district administration may develop appropriate user notification forms, guidelines and procedures necessary to implement this policy for submission to the school board for information. These guidelines, forms and procedures will be an addendum to this policy.
B. The administration will revise the user notifications, including student and parent notifications, if necessary, to reflect the adoption of these guidelines and procedures.
C. The district educational technologies policy is available for review by parents, employees and members of the community.
D. Due to the rapid evolution in educational technologies, the school board will conduct an annual review of this policy.

Legal References:
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. § 6751 *et seq.* (Enhancing Education Through Technology Act of 2001)
47 U.S.C. § 254 (Children's Internet Protection Act)
47 C.F.R. § 54.520 (FCC rules implementing CIPA)
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)
Tinker v. Des Moines Indep. Cmty. Sch. Dist., 393 U.S. 503 (1969)
United States v. American Library Association, 539 U.S. 194 (2003)
Tatro v. Univ. of Minnesota, 800 N.W.2d 811 (Minn. App. 2011)
Layshock v. Hermitage Sch. Dist., 650 F.3d 205 (3rd Cir. 2011)
J.S. v. Bethlehem Area Sch. Dist., 807 A.2d 847 (Pa. 2002)

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)
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 Records)
MSBA/MASA Model Policy 519 (Interviews of Students by Outside Agencies)
MSBA/MASA Model Policy 521 (Student Disability Nondiscrimination)
MSBA/MASA Model Policy 522 (Student Sex Nondiscrimination)
MSBA/MASA Model Policy 603 (Curriculum Development)
MSBA/MASA Model Policy 604 (Instructional Curriculum)
MSBA/MASA Model Policy 606 (Textbooks and Instructional Materials)

MSBA/MASA Model Policy 806 (Crisis Management Policy)
MSBA/MASA Model Policy 904 (Distribution of Materials on School District Property by Nonschool Persons)

Adopted 6/16
Revised 08/22

Appendix I

ONLINE CODE OF ETHICS (STUDENTS AND STAFF)

In the Park Rapids 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 products including but not limited to blogs, wikis, podcasts, Google applications and Moodle for student assignments are required to keep personal information out of their postings.
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 as another classmate.
4. Students using Web 2.0 tools will treat these tools as a classroom space. Speech that is inappropriate for class is not appropriate on Web 2.0 tools. Students are expected to treat others and their ideas online with respect.
5. Assignments on Web 2.0 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 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 a blog or other Web 2.0 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 Web 2.0 tools from home or school, using school equipment, will 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 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.
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. School board policies concerning acceptable use of electronic technology include the use of these Web 2.0 tools for school.
13. Failure to follow this code of ethics will result in academic sanctions and/or disciplinary action.

Revised: 7/24/13

Appendix II

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 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 student
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. Do not discuss students, their families or coworkers.
7. Student images obtained from your employment with the 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. 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 Park Rapids Area Schools." An employee in a leadership role in the

district, by virtue of his or her position, must consider whether personal thoughts he or she publishes will be attributed to this district.

10. Social media identifications, login identifications, and user names must not contain the district's name or logo without prior written permission from District Administration

Revised: 7/24/13

Appendix III

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. Teachers may also elect to use other social media tools for the purpose of instruction in accordance with Policy – 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 Park Rapids Area Schools.
    3. The teacher must not disclose information on any online social media site that is district property, protected by data privacy laws, or in violation of copyright.

A. Nondistrict Social Media Tools
    1. If a teacher elects to use a nondistrict social media tool, the teacher must build a separate page in that social media tool from his or her 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 Park Rapids Public Schools.
    5. The teacher 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 from District Administration

Appendix IV

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; and
6. Plan for monitoring site, addressing policy violations, and ensuring current content.

The request should be submitted to the Superintendent and building Principal. 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 Superintendent and building Principal 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 – Electronic Technologies Acceptable Use Policy Handbook and record retention requirements.

Revised: 7/24/13

Appendix V

GUIDELINES FOR DISTRICT FACEBOOK PAGE

The District's Facebook presence creates an accessible communications outlet, providing district news, facilitating district-related discussion by the community, and guiding viewers to departmental websites at www.parkrapids.k12.mn.us. These guidelines are used in conjunction with Policy (Electronic Technologies Acceptable Use) and all other district policies.

Establishment of Page:

1. The District will include on its Facebook page, in a prominent location, a link to the Park Rapids Area 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:
4. This page is intended to serve as a mechanism for communication between the public and Park Rapids Area Schools. Any comments submitted to this page, and its list of fans, are public records subject to disclosure and retention pursuant to Minnesota law. Public disclosure requests must be directed to Park Rapids Area Schools.
5. The communications department will be responsible for monitoring the district Facebook page, including content and comments, to ensure compliance with guidelines for use as posted on the Facebook page.

Postings:
The District will provide balance in topics shared on its Facebook webpage. 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 director of communications.

Revised: 7/24/12

Appendix VI

STUDENT ONLINE ACCEPTABLE USE CONSENT FORM

Grade_____ Graduation Year_____ Advisor/Teacher_____

Student

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

Student Name (PRINT) _____

Student's Signature_____

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 Park Rapids Area 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.

Parent/Guardian Name (PRINT) _____

Signature of Parent/Guardian_____

Date_____

Return this form to your school's Office.

Revised:5/17/16

Appendix VII

EMPLOYEE ONLINE ACCEPTABLE USE CONSENT FORM

I understand and will abide by the Park Rapids Area School District 309 Acceptable Use Policy. All use of the District 309's computers and Internet shall be consistent with District 309's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. This Authorization does not attempt to state all required or proscribed behavior by users. However, some specific examples are provided. The failure of any user to follow the terms of the Authorization for Computer use, Local Area Network use and Internet Access will result in the loss of privileges, disciplinary action, and/or appropriate legal action. The signature(s) at the end of this document is legally binding and indicates the party who signed has read the terms and conditions carefully and understands their significance.

All computer use can be monitored, including e-mail, to see that the accounts are being used for the stated purposes. For this and other reasons, e-mail is not private. The district also uses remote management and remote viewing tools, with the ability to remotely take control and view any workstation on the network. Information Technology (IT) can use remote management and viewing at any time, and may at times inconvenience users. We will do our utmost to minimize disruptions.

By signing this authorization, users understand they allow remote access and remote viewing and will not disconnect any Information Technology technician from your workstation at any time.

Access to District 309's Network and Internet must be for the purpose of education or research, and be consistent with the educational objectives of District 309.

Privileges: The use of District 309's computers and Internet is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges. The Director of Information Technology, and/or the building principal and School Administration will make all decisions regarding whether or not a user has violated this Authorization and may deny, revoke, or suspend access at any time. His or her decision is final.

Unacceptable Use: You are responsible for your actions and activities involving Internet use and the network.

a. Using the network for any illegal activity, including violation of copyright or other contracts, sending threatening messages, engaging in child pornography or transmitting any material in violation of any U.S. or State regulation;
b. Unauthorized downloading or copying software;
c. Downloading copyrighted material for other than personal use;
d. Using the network for private financial or commercial gain;
e. Wastefully using resources, such as file space;
f. Gaining unauthorized access to resources or entities;
g. Invading the privacy of individuals;
h. Using another user's account or password;
i. Posting material authored or created by another without his/her consent;
j. Chatting (live-time communication)
k. Viewing, downloading or printing obscene or inappropriate materials
l. Failing to report known violations
m. Using Novell instant messenger, send or broadcast any message on the Local Area Network or Wide Area Network
n. Using the network for commercial or private advertising;
o. Accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal material; and
p. Using the network while access privileges are suspended or revoked.

Network Etiquette: You are expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:

a. Be polite. Do not become abusive in your messages to others;
b. Use appropriate language. Do not swear, or use vulgarities or any other inappropriate language;
c. Do not reveal the personal addresses or telephone numbers of students or colleagues;
d. Recognize that electronic mail (E-Mail) is not private. People who operate the system have access to all mail. Messages relating to or in support of illegal activities may be reported to the authorities;
e. Do not use the network in any way that would disrupt its use by other users.
f. Consider all communications and information accessible via the network to be private property.

No Warranties: District 309 makes no warranties of any kind, whether expressed or implied, for the service it is providing. District 309 will not be responsible for any damages you suffer. This includes loss of data resulting from delays, non-deliveries, missed deliveries, or service interruptions caused by its negligence or your errors or omissions. Use of any information obtained via the

Internet is at your own risk. District 309 specifically denies any responsibility for the accuracy or quality of information obtained through its service.

Equipment: In order to encourage the integration of technology into curriculum and promote the acquisition and maintenance of technology skills, the Park Rapids Area Schools allows employees to use district computer technology off of District 309 property. This may include the use of district-owned personal computers, tablets, printers, and other devices. The equipment being used at a personal residence must not be used in any manner that will violate any local, state or federal law or the district policy.

Legal ownership of the equipment remains with the District. Employees will return the technology equipment and accessories at the time of termination of employment. The District reserves the right to repossess equipment and accessories at any time. The District may also choose to limit and/or withdraw home use privileges for failure to comply. Failure to return the property in a timely fashion may result in the involvement of law enforcement.

Indemnification: The user agrees to indemnify District 309 for any losses, costs, or damages, including reasonable attorney fees, incurred by District 309 relating to, or arising out of, any breach of the Authorization.

Security: Network security is a high priority. If you can identify a security problem on the Internet, you must notify the system administrator or the Director of Information Technology. Do not demonstrate the problem to other users. Keep your account and password confidential. Do not use another individual's account. Attempts to log-on to the Internet as a system administrator will result in cancellation of user privileges. Any user identified as a security risk may be denied access to the network.

Vandalism: Vandalism will result in cancellation of privileges and other disciplinary action. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the Internet, or any other network. This includes, but is not limited to, the uploading, downloading or creation of computer viruses.

Employee

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

Employee Name (PRINT) _____

Employee's Signature_____

School Building_____

Date_____

Return this form to the District Office.

Revised:5/17/16