No.524

NETWORK SYSTEM AND INTERNET ACCEPTABLE USE

I. PURPOSE

The purpose of this policy is to set forth policies and guidelines for access to the School District network and information systems, cloud based services, and acceptable and safe use of the Internet, including electronic communications.

II. GENERAL STATEMENT OF POLICY

In making decisions regarding student, employee and all account users, including guest access, to the School District network and information system and the Internet, including electronic communications**,** the School District considers its own stated educational mission, goals, and objectives. Electronic information, storage systems, and research skills are now fundamental to preparation of citizens and future employees. Access to the School District network system, storage systems, and to the Internet enables students and employees to explore thousands of libraries, databases, bulletin boards, and other resources while exchanging messages, and collaborating with people around the world. The School District expects that faculty will blend thoughtful use of the School District network system and the Internet throughout the curriculum and will provide guidance and instruction to students in their use.

III. LIMITED EDUCATIONAL PURPOSE

The School District is providing students, employees, limited account users, including guests, with access to the School District network and information system, and cloud-based service, which includes Internet access. The purpose of the system is more specific than providing students and employees with general access to the Internet. The School District system has a limited educational purpose, which includes use of the system for classroom activities, educational research, and professional or career development activities. Users are expected to use network, storage systems and Internet access through the district system to further educational and personal goals consistent with the mission of the School District and school policies. Uses that might be acceptable on a user's private personal account on another system may not be acceptable on this limited- purpose network.

IV. USE OF SYSTEM IS A PRIVILEGE

The use of the School District system and access to use is a privilege, not a right. Depending on the nature and degree of the violation and the number of previous viola- tions, unacceptable use of the School District storage systems, 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.

V. UNACCEPTABLE USES

A. The following uses of the School District system and Internet resources or accounts are considered unacceptable:

1. Users will not use the School District system to access, review, upload, download, complete, store, print, post, receive, transmit or distribute:

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

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

c. video streams, sound bites, music, radio feeds, and other media forms that use a high capacity of bandwidth. Exceptions may be made if used for instructional purposes;

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 School District system to knowingly or recklessly post, transmit or distribute false or defamatory information about a person or organization, or to harass another person, or to engage in personal attacks, including prejudicial or discriminatory attacks.

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

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

5. Users will not use the School District 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. Attempts to log on to the Internet as a system administrator will result in cancellation of user privileges and forwarding of the breach attempt to authorities. Any user identified as a security risk may be denied network access or have limited privileges.

6. Users will not trespass in another person's folders, work, files, or data content.

7. Users must not deliberately or knowingly delete a student or employee file.

8. Users will not use the School District system to post or distribute 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 or communications between employees and other individuals when such communications are made for education-related purposes (i.e., communications with parents or other staff members related to students).

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

c. These prohibitions specifically prohibit a user from utilizing the school district system to post personal information about a user or another individual on social networks, including, but not limited to, social networks such as “Twitter”, “Instagram”, “Snapchat”, and “Facebook.”

9. All account information and passwords are kept on file with the School District’s Technology Department. Users will not attempt to gain unauthorized access to the School District system or any other system through the School District system, attempt to log in through another person’s account, or use network/computer accounts, access codes or network identification other than those assigned to the user. Messages and records on the School District system may not be encrypted without the permission of appropriate school authorities.

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

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

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

B. An account user, guest, 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. Examples of such violations are, but are not limited to, situations where the school district 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, electronic device or resource, the school district may investigate such reports to the best of its ability. Account users, guests, 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 network system and the Internet and discipline under other appropriate school district policies, including suspension, expulsion, exclusion, or termination of employment.

C. If a user inadvertently accesses unacceptable materials or an unacceptable Internet site, the user shall 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, director of technology, or network administrator. This disclosure may serve as a defense against an allegation that the user has intentionally violated this policy.

VI. FILTER

A. With respect to any District-owned computers/devices connected to the District network for Internet access and off the District Network, 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. All School District computers and devices connected to the District network for Internet access will restrict, by use of available software filtering technology or other effective methods, all access to materials that are reasonably believed to be obscene, child pornography or harmful to minors under state or federal law.

B. The term “harmful to minors” means any picture, video, 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. Notification will be given that the district shall use 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.

E. Software filtering technology shall be narrowly tailored and shall not discriminate based on viewpoint.

VII. 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 District accessible 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, internet site activity, e-mail files and instant messaging content using District-owned electronic devices. In addition, all system users, including 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 Minnesota Statutes, Chapter 13 (the Minnesota Government Data Practices Act). Note that e-mail, chat, google searching is not guaranteed to be private. People who operate the system have access to all mail, searching, and browsing history.

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.

VIII. 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. Guest users and employees using the network system and Internet on District-owned electronic devices must sign the Internet Use Agreement. 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.

D. The District will use every opportunity to educate minors about appropriate online behavior and responsible citizenship including interacting and collaborating with other individuals on projects, social networking and cyber bullying awareness and response. This includes monitoring the online activities of minors and teaching online safety to students.

IX. LIMITATION ON SCHOOL DISTRICT LIABILITY

Use of the School District system is at the user's own risk. The system is provided on an "as is, as available" basis. The 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 content management systems (storage devices such as CD/DVD, flash memory) diskettes, tapes, hard drives or servers, or for delays or changes in or interruptions of service or misdeliveries or nondeliveries of information or materials, regardless of the cause. The School District is not responsible for the accuracy or quality of any advice or information obtained through or stored on the School District system. The School District will not be responsible for financial obligations arising through unauthorized use of the School District system or the Internet.

X. USER NOTIFICATION

A. All users shall be notified of the School District policies relating to Network System and Internet Acceptable Use annually

B. This notification shall include the following:

1. Notification that Internet use is subject to compliance with School District policies.

2. Disclaimers limiting the School District's liability relative to:

    a. Information stored on School District storage devices, hard drives or servers.

    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 network accounts.

4. Notification that, even though the School District may use technical means to limit user Network or 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 user and/or the minor's parents.

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.

XI. 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 Internet and the School District system 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 cloud services, the Internet and that the School District will provide parents the option to request alternative activities not requiring storage or 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 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.

XII. BRING YOUR OWN DEVICE (BYOD)

A. The Bring Your Own Device (BYOD) option has a limited educational purpose. Therefore, BYOD participants are expected to use the privilege to further educational goals consistent with the mission of the Monticello Public School District and school district policies.

B. The Monticello School District, to be consistent with the Federal Children's Internet Protection Act, prohibits students, staff and guests from using outside networks and the capability of 3G or 4G internet networks while at school.

C. The Monticello School District will allow students, staff and guests to access MAGICNET wireless network using their own technology devices (laptops, SmartPhones, iPads, etc.) during the school day. With classroom teacher approval, student may use their own devices in the classroom to access and save information from the Internet, communicate with other learners and use the productivity tools loaded on the devices. ISD882 will not provide software or district owned productivity tools to personal devices or non-district owned devices.

D. Users will be prompted to accept the following terms of use prior to each attempt at connecting to MAGICNET:

1. Any user accessing the Monticello Public Schools MAGICNET wireless network agrees to comply with the District's standards and is given filtered access to the Internet only. Users will be granted access only if he or she accepts the District's Internet Acceptable Use and Safety Policy and access to the Internet will be granted in accordance with the Internet Acceptable Use and Safety Policy.

2. Applicability of Other Policies: This document is part of the Monticello Public Schools #882's cohesive set of School Board policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

3. Security Considerations

a. Wireless access is by nature an insecure medium. As with most guest wireless networks, any information being sent or received over the Monticello Public Schools MAGICNET wireless network could potentially be intercepted by another wireless user. Cautious and informed wireless users should not transmit their credit card information, passwords and any other sensitive personal information while using a wireless "hot spot".

b. Anyone using the Monticello Public Schools MAGICNET wireless network is forewarned that there can be no expectation of privacy when using the wireless network. Users assume all associated risks and agree to hold harmless the Monticello Public Schools #882 and its employees for any personal information (e.g. credit card) that is compromised, or for any damage caused to users' hardware or software due to electric surges, security issues or consequences caused by viruses or hacking. All wireless access users should have up-to-date virus protection on their personal laptop computers or wireless devices, as well as staying up-to-date with applicable OS security patches.

4. Disclaimer

a. The Monticello Public Schools #882 is providing wireless connectivity in this facility as a guest service and offers no guarantees that any use of the wireless connection is in any way secure, or that any privacy can be protected when using this wireless connection. Use of this wireless connection is entirely at the risk of the user, and the Monticello Public Schools #882 is not responsible for any loss of any information that may arise from the use of the wireless connection, or for any loss, injury, or damages resulting from the use of the wireless connection.

.

E. Students and staff who do not accept the terms of service will not be able to access the MAGICNET wireless network. The terms of service prompt will post each time the user initiates a connection to this wireless network. Once on the MAGICNET network, all users will have filtered Internet access just as they would on a district owned device.

Adopted: 11/20/00

Revised:	12/03/01	Reviewed: 07/11/11	Revised: 04/04/19
	06/16/08	07/02/12	
	07/13/09	Revised: 12/09/13	
	06/07/10	04/07/15	