Adopted:	February 9, 2015
School Board Revised:	November 22, 2021 [MSBA Model Policy/Modified/Mandatory]
School Board Revised:	February 27, 2023 [Routine Review/No Change]
School Board Review:	February 26, 2024 [Routine Review/No Change]
School Board Approval:	March 18, 2024 [Routine Review/No Change]
Contact Person:	Executive Director of Technology and Information Services

POLICY 524 COMPUTER SYSTEM AND INTERNET ACCEPTABLE USE

I. PURPOSE:

To set forth policies and Regulations for access to the district computer system and acceptable and safe use of the Internet, including electronic communications.

II. GENERAL POLICY STATEMENT

Administration will develop and enforce regulations to ensure the security of the district computer system and the safety of students and staff using the district computer system. These regulations support:

A. Access and use of the district computer system and the Internet, including electronic communication, must align with the District Strategic Plan.

B. The District expects that faculty will blend thoughtful use of the district computer system and the Internet throughout the curriculum and will provide guidance and instruction to students in their use.

C. Internet access and use is for educational purposes.

D. The use of the district computer system and access to use of the Internet is a privilege, not a right. Depending on the nature and the degree of the violation and the number of previous violations, unacceptable use may result in consequences to be determined by the District.

E. District information on the district computer system is the property of the District and unauthorized accessing and altering of this data is prohibited.

F. The district communication system is for school business use only.

Adopted: February 9, 2015
School Board Revised: November 22, 2021 [MSBA Model Policy/Modified/Mandatory]
School Board Revised: February 27, 2023 [Routine Review/No Change]
School Board Review: February 26, 2024 [Routine Review/No Change]
School Board Approval: March 18, 2024 [Routine Review/No Change]

Contact Person: Executive Director of Technology and Information Services

REGULATION 524 COMPUTER SYSTEM AND INTERNET ACCEPTABLE USE

I. UNACCEPTABLE USES

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

1. Users will not use the district system to 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 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 the creation of impersonating or fake accounts, prejudicial or discriminatory attacks.

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

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

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

6. Users will not use the district system to post private information about another person, personal contact information about themselves or other persons, or other personally identifiable information except for education-related purposes.

7. Users must keep all account information and passwords on file with the designated district official. Users will not attempt to gain unauthorized access to the district system or any other system through the district system, attempt to log in through another person's account, or use computer accounts, access codes or network identification other than those assigned to the user. Messages and records on the district system may not be encrypted without the permission of appropriate school authorities.

8. Users will not use the district system to violate copyright laws or usage licensing agreements, or otherwise to use another person's property without the person's prior approval or proper citation.

9. Users will not use the district system for conducting business, for unauthorized commercial purposes or for financial gain unrelated to the mission of the District. Users will not use the district system to offer or provide goods or services or for product advertisement.

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

B. A student or staff engaging in any of the foregoing unacceptable uses of the Internet when off district premises and without the use of the district system also may be in violation of this policy as well as other district policies. If the District receives a report of an unacceptable use originating from a non-school computer or resource, the District shall investigate such reports to the best of its ability. Students or staff may be subject to disciplinary action under other appropriate district policies, including suspension, expulsion, exclusion, or termination of employment.

C. If a user inadvertently accesses unacceptable materials or an unacceptable Internet site, the user shall immediately disclose the inadvertent access to an appropriate district official. In the case of staff, the immediate disclosure shall be to the staff member'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 with appropriate guidance from the appropriate teacher or, in the case of staff, the building administrator or designee.

II. FILTER

A. With respect to any of its computers with Internet access, the 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 to minors.

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

D. 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.

E. The District will educate students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.

III. CONSISTENCY WITH OTHER SCHOOL POLICIES

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

IV. LIMITED EXPECTATION OF PRIVACY

A. 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. Users should expect only limited privacy in the contents of personal files on the district system.

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

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

D. Parents and caregivers have the right at any time to investigate or review the contents of their minor child's files and email files to the extent that it does not violate the privacy policy of the District.

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

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

V. ELECTRONIC RECORD RETENTION – EMAIL MESSAGES

Email messages are potentially official government records. All email messages that fall under the "correspondence" category will be archived according to the School District General Records Retention Schedule of the State of Minnesota.

District email is stored for a period of three years from date of receipt through a backup process. The archiving of messages deemed as official records beyond three years will be the responsibility of the individual users. Any message can be retrieved during that time period.

VI. INTERNET USE REGULATIONS

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/caregivers and staff of the District. Technology tools, including appropriate use of the Internet, are expected components of the Bloomington learning experience.

B. The Internet Use Regulations are published in student and faculty handbooks. These regulations are reviewed on a regular basis. It is the parent/caregiver's responsibility to be knowledgeable of the published Internet Use Regulations.

VII. LIMITATION ON DISTRICT LIABILITY

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

VIII. USER NOTIFICATION

All users shall be notified of the district policies relating to Internet use at time of employment, and through student and staff handbooks.

IX. PARENT/CAREGIVER RESPONSIBILITY

Outside of school, parents/caregivers bear responsibility for the same guidance of Internet use as they exercise with other information sources. Parents/Caregivers are responsible for monitoring their student's use of the district system and of the Internet if the student is accessing the district system from home or a remote location.

X. NOTIFICATION REGARDING TECHNOLOGY PROVIDERS

A. Within 30 days of the start of each school year, the District must give parents/caregivers 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.

B. The District must provide parents/caregivers and students an opportunity to inspect a complete copy of any contract with a technology provider.

C. A contract between a technology provider and the District must include requirements to ensure appropriate security safeguards for educational data.

D. 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.

XI. SCHOOL-ISSUED DEVICES

A. Except as provided in paragraph B, the District or a technology provider must not electronically access or monitor: any location-tracking feature of a school-issued device; any audio or visual receiving, transmitting, or recording feature of a school-issued device; or student interactions with a school-issued device, including but not limited to keystrokes and web-browsing activity.

B. The District or a technology provider may only engage in activities prohibited by paragraph A if: the activity is limited to a noncommercial educational purpose for instruction, technical support, or exam-proctoring by staff, student teachers, staff contracted by the District, a vendor, or the Minnesota Department of Education, and notice is provided in advance; the activity is permitted under a judicial warrant; the District is notified or becomes aware that the device is missing or stolen; the activity is necessary to respond to an imminent threat to life or safety and the access is limited to that purpose; the activity is necessary to comply with federal or state law, including but not limited to Minnesota Statutes section 121A.031; or the activity is necessary to participate in federal or state funding programs, including but not limited to the E-Rate program.

C. If the District or a technology provider interacts with a school-issued device as provided in paragraph B, it must, within 72 hours of the access, notify the student to whom the school-issued device was issued or that student's parent or caregiver.

XII. 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.

XIII. IMPLEMENTATION

A. The Administration shall develop appropriate user notification forms, Regulations , and procedures necessary to implement this policy.

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

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

D. Because of the rapid changes in the development of the Internet, the School Board shall conduct an annual review of this policy.