

Adopted: 9/9/1999

Orig. 1996

Rev. 2022

Revised: 8/18/2022

524 INTERNET ACCEPTABLE USE AND SAFETY POLICY

I. PURPOSE

The purpose of this policy is to set forth policies and guidelines for access to the school district computer system and acceptable and safe use of the Internet, including electronic communications.

II. GENERAL STATEMENT OF POLICY

In making decisions regarding student and employee access to the school district computer system and the Internet, including electronic communications, the school district considers its own stated educational mission, goals, and objectives. Electronic information research skills are now fundamental to preparation of citizens and future employees. Access to the school district computer system and to the Internet enables students and employees to explore thousands of libraries, databases, websites and other resources while connecting with people around the world. The school district expects that faculty will blend thoughtful use of the school district computer 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 and employees with access to the school district computer system, which includes Internet access. The purpose of the system is more specific than providing students and employees with general access to the Internet. The 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 Internet access through the district system to further educational and personal goals consistent with the mission of the school district and school policies. Uses which might be acceptable on a user's private personal account on another system may not be acceptable on this limited-purpose network.

IV. USE OF SYSTEM IS A PRIVILEGE

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

V. UNACCEPTABLE USES

A. While not an exhaustive list, 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, store, print, post, receive, transmit, or distribute:
 - a. pornographic, obscene, or sexually explicit material or other visual depictions that are deemed by the district to be inappropriate and/or otherwise 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 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 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.
6. Users will not use the school district system to post private information about another person, personal contact information about themselves or other persons, or other personally identifiable information, including, but not limited to, addresses, telephone numbers, school addresses, work addresses, identification numbers, account numbers, access codes or passwords, labeled photographs, or other information that would make the individual's identity easily traceable, and will not repost a message that was sent to the user privately without permission of the person who sent the message.
 - a. This paragraph does not prohibit the posting of employee contact

information on school district webpages 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 personal contact information about themselves on a webpage. However, employees may not post personal contact information or other personally identifiable information about students unless:
 - (1) such information is classified by the school district as directory information and verification is made that the school district has not received notice from a parent/guardian or eligible student that such information is not to be designated as directory information in accordance with Policy 515; or
 - (2) such information is not classified by the school district as directory information but written consent for release of the information to be posted has been obtained from a parent/guardian or eligible student in accordance with Policy 515.

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

- c. These prohibitions specifically prohibit a user from utilizing the 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 “Facebook,” “Twitter,” “Instagram,” “Snapchat,” “TikTok” “Reddit,” and similar websites or applications.
- 7. 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 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.
 - 8. Users will not use the school district system to violate copyright laws or usage licensing agreements, or otherwise to use another person’s property without the person’s prior approval or proper citation, including the downloading or exchanging of pirated software, music or video, or copying software to or from any school computer, and will not plagiarize works they find on the Internet.
 - 9. 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.

10. Users will not use the school district system to engage in bullying or cyberbullying in violation of the school district's Bullying Prohibition Policy (ISD #139 Policy 514). This prohibition includes using any technology or other electronic communication off school premises to the extent that student learning or the school environment is substantially and materially disrupted.
- B. A student or employee 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 may include, 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 or resource, the school district may investigate such reports to the best of its ability. Students or employees may be subject to disciplinary action for such conduct, including, but not limited to, suspension or cancellation of the use or access to the school district computer system and the Internet and discipline under other appropriate school district policies, including suspension, expulsion, exclusion, or termination of employment.
 - C. If a user inadvertently accesses unacceptable materials or an unacceptable Internet site, the user shall immediately disclose the inadvertent access to an appropriate school district official. In the case of a school district employee, the immediate disclosure shall be to the employee's immediate supervisor and/or the building administrator. This disclosure may serve as a defense against an allegation that the user has intentionally violated this policy. In certain rare instances, a user also may access otherwise unacceptable materials if necessary to complete an assignment and if done with the prior approval of and with appropriate guidance from the appropriate teacher or, in the case of a school district employee, the building administrator.

VI. FILTER

- A. With respect to any of its computers with Internet access, and personal devices accessing the schools guest wifi network, the school district will follow the guidelines provided by the Children's Internet Protection Act (CIPA), and will monitor the online activities of users and employ technology protection measures during any use of such computers by minors and adults. The technology protection measures utilized will block or filter Internet access to any visual depictions that are:
 1. Obscene;
 2. Child pornography; or
 3. Harmful to minors.
- B. The term "harmful to minors" means any picture, image, graphic image file, or other visual depiction that:
 1. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; or
 2. Depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or

simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and

3. Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.
- C. 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 school district will educate students about appropriate online behavior (Digital Citizenship), including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.

VII. CONSISTENCY WITH OTHER SCHOOL POLICIES

- A. Use of the school district computer system and use of the Internet shall be consistent with school district policies and the mission of the school district.
- B. Students who are permitted to bring their own electronic devices to school will comply with school specific guidelines for the use of personal electronic devices in school.

VIII. 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/Guardians 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.

IX. INTERNET USE AGREEMENT

- A. The proper use of the District Electronic Technologies and Internet, and the educational value to be gained from proper Internet use, is the joint responsibility of students, parents/guardians, and employees of the school district.
- B. This policy requires the permission of and supervision by the school's 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.
- D. All users shall be responsible for the protection and security of their passwords. Staff shall have the ability to change passwords and maintain the confidentiality of logon codes.
- E. Students are never allowed to use a Staff computer.
- F. Computers / computer terminals shall not be left logged-on when unattended and shall be password-protected. Screens can be locked with the Windows + L keys. (Clear Desk and Clear Screen Procedure)
- G. Where practically possible, paper and computer media shall be stored in suitable locked safes, cabinets or other forms of security furniture when not in use, especially outside working hours.
- H. Sensitive or classified information, when printed, shall be cleared from printers immediately.

X. 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 hard drives, servers or hosted services 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.

XI. USER NOTIFICATION

- A. All users shall be notified of the school district policies relating to Internet use.
- 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, hard drives, servers, or hosted services.
 - b. Information retrieved through school district computers, networks, or online resources.
 - c. Personal property used to access school district computers, networks, or online resources.
 - d. Unauthorized financial obligations resulting from use of school district resources/accounts to access the Internet.
3. A description of the privacy rights and limitations of school sponsored/managed Internet accounts.
4. Notification that, even though the school district may use technical means to limit student Internet access, these limits do not provide a foolproof means for enforcing the provisions of this acceptable use policy.
5. Notification that goods and services can be purchased over the Internet that could potentially result in unwanted financial obligations and that any financial obligation incurred by a student through the Internet is the sole responsibility of the student and/or the student's parents.
6. Notification that the collection, creation, reception, maintenance, and dissemination of data via the Internet, including electronic communications, is governed by Public and Private Personnel Data Policy, and Protection and Privacy of Pupil Records Policy.
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.
9. Notification that student email addresses may be provided to District approved third-party providers for access to educational tools and content.

XII. 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. This notification should include:

1. A copy of the user notification form provided to the student user.
2. A description of parent/guardian responsibilities.
3. A notification that the parents/guardians have the option to request alternative educational activities not requiring Internet access and the material to exercise this option.
4. A statement that the Internet 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/guardian to review.

XIII. IMPLEMENTATION; POLICY REVIEW

- A. The school district administration may develop appropriate user notification forms, guidelines, and procedures necessary to implement this policy for submission to the school board for approval. Upon approval by the school board, such guidelines, forms, and procedures shall be an addendum to this policy.
- B. The administration shall revise the user notifications, including student and parent notifications, if necessary, to reflect the adoption of these guidelines and procedures.
- C. The school district Internet policies and procedures are available for review by all parents, guardians, staff, and members of the community.
- D. Because of the rapid changes in the development of the Internet, the school board shall conduct an annual review of this policy.

Legal References: Minn. Stat. Ch. 13 (Minnesota Government Data Practices Act)
15 U.S.C. § 6501 *et seq.* (Children's Online Privacy Protection Act)
17 U.S.C. § 101 *et seq.* (Copyrights)
20 U.S.C § 1232g (Family Educational Rights and Privacy Act)
47 U.S.C. § 254 (Children's Internet Protection Act of 2000 (CIPA))
47 C.F.R. § 54.520 (FCC rules implementing CIPA)
Minn. Stat. § 121A.031 (School Student Bullying Policy)
Minn. Stat. § 125B.15 (Internet Access for Students)
Minn. Stat. § 125B.26 (Telecommunications/Internet Access Equity Act)
Mahanoy Area Sch. Dist. v. B.L., 594 U.S., 141 S. Ct. 2038 (2021)
Tinker v. Des Moines Indep. Cmty. Sch. Dist., 393 U.S. 503,
United States v. Amer. Library Assoc., 539 U.S. 194, 123 S.Ct. 2297, 56 L.Ed.2d
221 (2003)
Sagehorn v. Indep. Sch. Dist. No. 728, 122 F.Supp.2d 842 (D. Minn. 2015)
R.S. v. Minnewaska Area Sch. Dist. No. 2149, 894
F.Supp.2d 1128 (D. Minn. 2012)
Tatro v. Univ. of Minnesota, 800 N.W.2d 811 (Minn. App. 2011), *aff'd* on other

grounds 816 N.W.2d 509 (Minn. 2012)
S.J.W. v. Lee's Summit R-7 Sch. Dist., 696 F.3d 771 (8th Cir. 2012)
Parents, Families and Friends of Lesbians and Gays, Inc. v. Camdenton R-III Sch. Dist., 853 F.Supp.2d 888 (W.D. Mo. 2012)
M.T. v. Cent. York Sch. Dist., 937 A.2d 538 (Pa. Commw. Ct. 2007)

Cross References: ISD #139 Policy 403 (Discipline, Suspension, and Dismissal of School District Employees)
ISD #139 Policy 406 (Public and Private Personnel Data)
ISD #139 Policy 505 (Distribution of Nonschool-Sponsored Materials on School Premises by Students and Employees)
ISD #139 Policy 506 (Student Discipline)
ISD #139 Policy 514 (Bullying Prohibition Policy)
ISD #139 Policy 515 (Protection and Privacy of Pupil Records)
ISD #139 Policy 519 (Interviews of Students by Outside Agencies)
ISD #139 Policy 521 (Student Disability Nondiscrimination)
ISD #139 Policy 522 (Title IX Sex Nondiscrimination Grievance Procedures and Process)
ISD #139 Policy 603 (Curriculum Development)
ISD #139 Policy 604 (Instructional Curriculum)
ISD #139 Policy 606 (Textbooks and Instructional Materials)
ISD #139 Policy 806 (Crisis Management Policy)
ISD #139 Policy 904 (Distribution of Materials on School District Property by Nonschool Persons)

Rush City Schools Computer and Internet Use Agreement

Rush City Schools provides students and employees with access to the school district's computer system, which includes Internet access. The district system has a limited educational purpose, which includes use of the system for classroom activities, educational research, and professional or career development. Users are expected to use Internet access through the district system to further educational and personal goals consistent with the mission of the school district and school policies. Uses which might be acceptable on another system may not be acceptable on this limited-purpose network. Students, staff, and parents/guardians are encouraged to read School Board Policy #524, Internet Acceptable Use and Safety Policy. This policy is available in school offices and the District website, and it provides the basis for this agreement.

The computer resources in our schools must be used in ethical and lawful manner. Violations of School District computer policies, this Agreement, Internet etiquette, or violations of the laws of Minnesota and the United States can result in disciplinary action by Rush City Schools and/or prosecution by legal authorities. Access to computer systems and the Internet is a privilege. Individuals who sign this agreement, agree to abide by all of the expectations in Policy 524. Responsibilities and understandings include, but are not limited to, the following:

1. You must not permit others to use your account(s). You are responsible for maintaining the secrecy of all passwords you may have.
2. Communication that must be 100% secure and private should not be communicated via the Internet. Internet communications are not secure. Although security systems are in place to prevent unauthorized access, it is possible, although rare and difficult, for others to access your files.
3. Fraudulent, harassing, obscene, threatening and other inappropriate messages or uses of computers, networks, or the Internet must not be created, downloaded or transmitted. This includes any form of bullying or harassment of individuals or groups.
4. All information and references obtained through the use of technology systems must be attributed to the source. Plagiarism is expressly forbidden in all cases by the district.
5. Never give out personal or family information, such as phone numbers or addresses. Never arrange for a face-to-face meeting without parental/guardian supervision and never respond to abusive or suggestive messages. Report all such instances immediately to a member of the school staff.
6. Do not access or attempt to access, degrade, or disrupt systems or data that you are not authorized to access.
7. You may not install or download any software on school computers without written approval from a supervising teacher or the technology coordinator.
8. Making or distributing unauthorized or illegal copies of licensed software, music or video is against the law and can result in disciplinary action by your school district and/or prosecution by legal authorities.
9. School district computer technology and networks (including Internet) must not be used to promote products or services for the intent of financial or other gain unrelated to the mission of the school district.
10. The school district will not be responsible for damage or unavailability of data stored using district systems or for delays or disruptions in the systems. The school district is not responsible for the quality or accuracy of any information obtained through school district systems.
11. District technology personnel have access to all information, files, and email messages on district computers. Any unauthorized files or software may be removed without notice.
12. Parents/Guardians may review the contents of their child's files and/or request the termination of their child's account at any time.

COMPUTER AND INTERNET USE AGREEMENT - STUDENT

STUDENT

I have read and had an opportunity to discuss school district Policy 524 relating to safety and acceptable use of the school district computer system and the Internet and agree to abide by this policy. I further understand that should I commit any violation, my access privileges may be revoked, school disciplinary action may be taken, and/or appropriate legal action may be taken.

User's Full Name (please print): _____

User Signature: _____

Date: _____

PARENT OR GUARDIAN

As the parent or guardian of this student, I have read the school district Policy 524 relating to safety and acceptable use of the school district computer system and the Internet. I understand that this access is designed for educational purposes. The school district has taken precautions to eliminate controversial material. However, I also recognize it is impossible for the school district to restrict access to all controversial materials and I will not hold the school district or its employees or agents responsible for materials acquired on the Internet. Further, I accept full responsibility for supervision if and when my child's use is not in a school setting. I hereby give permission to issue an account for my child and certify that the information provided on this form is correct.

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

Parent or Guardian's Signature: _____

SUPERVISING TEACHER

(Must be signed if applicant is a student)

I have read the school district Policy 524 relating to safety and acceptable use of the school district computer system and the Internet and agree to promote these policy expectations with the student. Because the student may use the Internet on the school district computer system for individual work, or in the context of another class, I cannot be held responsible for the student's use of the Internet on network. As the supervising teacher I do agree to instruct the student on acceptable use of the Internet and network and proper network etiquette.

Teacher's Name (please print): _____

Teacher's Signature: _____

COMPUTER AND INTERNET USE AGREEMENT - EMPLOYEE

ISD #139 Computers, Networks, Internet Rights and Responsibilities Agreement

The computer resources and capabilities in our schools must be used in an ethical and lawful manner. Violations of the ISD # 139 computer policies, This Agreement, Internet etiquette, or violations of the laws of Minnesota and the United States can result in disciplinary action by ISD #139 and/or prosecution by legal authorities. Access to computer systems and the Internet is a privilege. Responsibilities include, but are not limited to, the following:

1. You must not permit others to use your account(s). You are responsible for maintaining the secrecy of all passwords you may have.
2. Fraudulent, harassing, obscene, threatening and other inappropriate messages or uses of computers, networks, dial access capabilities, or the Internet must not be created, downloaded or transmitted. This includes messages that might harass individuals or groups because of their age, race, gender, religious beliefs, sexual orientation, physical attributes, etc.
3. You must not access or attempt to access systems or data that you are not authorized to access. You must not use "loopholes" in computer security systems, "hacking", etc. or attempt to degrade performance or gain illegal access to computer systems and software.
4. Any references obtained through the use of technology systems must be attributed to the source. Plagiarism is expressly forbidden in all cases by the district.
5. Making or distributing unauthorized and illegal copies of licensed software is against the law and can result in disciplinary action by your school district and/or prosecution with severe legal penalties. Copyright laws will be strictly enforced on a case by case basis.
6. Your district's computer technology and networks (including Internet and dial access) must not be used to promote products or services for the intent or financial gain for yourself, your company or employer, or any other local enterprise.
7. You may not install any software on school computers without consent in writing from a sponsoring teacher, building media specialist or the technology coordinator.
8. Communication that must be 100% secure and private should not be communicated via the Internet. Internet communications are not secure. It is possible (although rare and difficult) for others to access your files, even though security systems are in place to prevent such access.
9. Never give out personal or family information, such as phone numbers or addresses. Never arrange for a face-to-face meeting without notifying your supervisor and/or co-workers and never respond to abusive or suggestive messages. Report all such instances immediately to your supervisor.
10. You must be able to demonstrate basic computer skills before you are allowed to use any school computer without direct supervision by another staff member.
11. District technology personnel shall have access to all files on district computers. Any unauthorized software or files may be removed without notice.

INTERNET USE AGREEMENT – EMPLOYEE

SCHOOL DISTRICT EMPLOYEE

I have read and do understand the school district Policy 524 relating to safety and acceptable use of the school district computer system and the Internet and agree to abide by this policy. I further understand that should I commit any violation, my access privileges may be revoked, school disciplinary action may be taken, and/or appropriate legal action may be taken.

User's Full Name (please print): _____

User Signature: _____

Date: _____