

VII. DISTRICT POLICY 524

Book	Rochester Public Schools Policies
Section	500 - STUDENTS
Title	Internet Acceptable Use and Safety Policy
Number	522
Status	Active
Legal	15 U.S.C. § 6501 et seq. (Children's Online Privacy Protection Act) 17 U.S.C. § 101 et seq. (Copyrights) 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) Tinker v. Des Moines Indep. Cmty. Sch. Dist., 393 U.S. 503, 89 S.Ct. 733, 21 L.Ed.2d 731 (1969) Minn. Stat. § 125B.26 (Telecommunications/Internet Access Equity Aid) United States v. Amer. Library Assoc., 539 U.S. 194, 123 S.Ct. 2297, 56 L.Ed.2d 221 (2003) Doninger v. Niehoff, 527 F.3d 41 (2nd Cir. 2008) R.S. v. Minnewaska Area Sch. Dist. No. 2149, No. 12-588, 2012 WL 3870868 (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) Kowalski v. Berkeley County Sch., 652 F.3d 565 (4th Cir. 2011) Layshock v. Hermitage Sch. Dist., 412 F.Supp. 2d 502 (W.D.Pa.2006)650 F.3d 205 (3rd Cir. 2011) 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	403 - Discipline, Suspension, and Dismissal of School District Employees 406 - Public and Private Personnel Data 505 - Distribution of Nonschool-Sponsored Materials on School Premises by Students 506 - Student Discipline 515 - Protection and Privacy of Pupil Records 519 - Interviews of Students by Outside Agencies 521 - Student Disability Nondiscrimination 522 - Student Sex Nondiscrimination 603 - Curriculum Development 604 - Instructional Curriculum 606 - Textbooks and Instructional Materials 806 - Crisis Management 904 - Distribution of Materials on School District Property by Non-school Persons
Adopted	June 20, 2006
Last Revised	July 27, 2021
Last Reviewed	May6, 2021

I. PURPOSE

The purpose of this policy is to establish requirements, expectations, and guidelines for access to the use of Electronic Technology.

II. DEFINITION

For purposes of this policy, the term "Electronic Technology" means all electronic systems, equipment, and devices that are owned, leased, or supplied by the School District, or are otherwise under the control of the School District, including, but not limited to, computers, computer systems, networks, hardware, software, electronic devices, electronic programs, electronic storage media, data bases, systems used to supply or facilitate Internet access, and Internet access provided by or gained through any School District service, system, device, or equipment. Personal devices are not supported on Rochester Public Schools systems. Connecting personal equipment to the district's secure network or installing personal software on any district-owned system is not permitted without prior approval from the technology department.

Personal devices may only be connected to the district's guest network/systems provided the personal devices comply with district standards and is compatible with the district's systems. Any devices attached to the district's network/systems are subject to the 524 Acceptable Use Policy and must adhere to the same policies and procedures as district owned equipment.

III. GENERAL STATEMENT OF POLICY

In making decisions regarding student and employee access to and use of Electronic Technology, the School District considers its own stated educational mission, goals, and objectives. The School District expects that staff will blend thoughtful use of Electronic Technology throughout the curriculum and will provide guidance and instruction to students in their use of such technology. Students and staff will be provided with opportunities to practice safe and ethical use of Electronic Technology at school to provide students with a relevant education. The School District may also use these tools and other communication technologies in fulfilling its responsibility for effectively communicating with the general public.

IV. LIMITED EDUCATIONAL PURPOSE

The School District is providing students and employees with access to Electronic Technology for education purposes. The School District system has a limited educational purpose, which include use of the system for classroom activities, educational research, and professional or career development activities. Users are expected to use Electronic Technology to further educational and professional goals consistent with the mission of the School District and school policies. Uses which might be acceptable on a user's private system may not be acceptable on Electronic Technology, which is owned, operated, or provided by the School District for a limited purpose.

V. USE OF SYSTEM IS A PRIVILEGE, NOT A RIGHT

Access to and use of Electronic Technology is a privilege, not a right. Depending on the nature and degree of the violation and the number of previous violations, unacceptable use of Electronic Technology may result in one or more of the following consequences: suspension or cancelation of use or access privileges; payments for damages and repairs; discipline under other appropriate School District policies, including suspension, expulsion, or exclusion;

reprimand, suspension, or termination of employment; censure or removal from the Board; or civil or criminal consequences or liability under other applicable laws.

VI. UNACCEPTABLE USES

A. The following uses of Electronic Technology are unacceptable:

1. Users may not use Electronic Technology 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 images, materials, language, or other data;
 - c. materials that use language or images that are inappropriate in the education setting or disruptive to the educational process;
 - d. materials that present a risk of harm to students, staff, Electronic Technology, or any School District property;
 - e. materials that may cause a material and substantial disruption to the educational process;
 - f. 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 may not use Electronic Technology 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. students are prohibited from audio or video recording on school property without prior permission from the principal or a teacher, and that permission will be granted only for an educational purpose
4. Users may not use Electronic Technology to engage in any illegal act or violate any local, state, or federal statute or law.
5. Users may not use Electronic Technology to vandalize, damage or disable the property of another person or organization, may not make deliberate attempts to degrade or disrupt equipment, software or system performance by spreading computer viruses or by any other means, may 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 may not use the School District Electronic Technology in such a way as to disrupt the use of the system by other users.
6. Users may not use Electronic Technology 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.
7. Users may not use Electronic Technology 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 may 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 (1) 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.

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 “MySpace” and “Facebook”, “Twitter”, “Instagram”, “Snapchat”, and “Reddit”, and similar websites or applications.

8. Users are responsible for complying with School District password security procedures. Users may not attempt to gain unauthorized access to Electronic Technology or any part of the School District’s electronic system or any other system through the School District system, attempt to log in through another person’s account, or user 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 (except by appropriate School District authorities for legal compliance).
 9. Users may not use Electronic Technology to violate copyright laws or usage licensing agreements, or otherwise to use another person’s property without the person’s prior approval or proper citation, including the downloading or exchanging of pirated software or copying software to or from any school computer, and may not plagiarize works they find on the Internet.
 10. Users may not use Electronic Technology for conducting business, for unauthorized commercial purposes or for financial gain unrelated to the mission of the School District. Users may not use the School District system to offer or provide goods or services or to advertise services or products without approval of the Superintendent or designee. Users may not use Electronic Technology to purchase goods or services for personal use without authorization from the appropriate School District official.
 11. Users will not use the school district system to engage in bullying or cyberbullying in violation of the school district’s Bullying Prohibition Policy (MSBA/MASA Model 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. This policy applies to the use of Electronic Technology regardless of whether or not the user is physically present on School District property and regardless of whether or not the user is attending a school sponsored event or activity.

- C. If a user inadvertently accesses unacceptable materials or an unacceptable Internet site, the user must immediately disclose the inadvertent access to an appropriate School District official. In the case of a School District employee, the immediate disclosure will be to the employee's immediate supervisor and/or the building administrator. 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.
- D. Any student or School District employee who witnesses unacceptable use of Electronic Technology is encouraged to report this unauthorized use to the appropriate School District official.

VII. FILTER

School districts which receive certain federal funding, such as e-rate discounts, for purposes of Internet access and connection services and/or receive funds to purchase Internet accessible computers are subject to the federal Children's Internet Protection Act, effective in 2001. This law requires school districts to adopt an Internet safety policy which contains the provisions set forth below. Also, the Act requires such school districts to provide reasonable notice and hold at least one public hearing or meeting to address the proposed Internet safety policy prior to its implementation. School districts that do not seek such federal financial assistance need not adopt the alternative language set forth below nor meet the requirements with respect to a public meeting to review the policy. The following alternative language for school districts that seek such federal financial assistance satisfies both state and federal law requirements.

- A. The School District may monitor the online activities of both minors and adults when those activities occur using Electronic Technology. The School District will employ technology protection measures. The technology protection measures utilized will see to block or filter Internet access to any visual depictions that are:
 - 1. Obscene;
 - 2. Child pornography;
 - 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;
 - 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;
 - 3. Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.
- C. Software filtering technology will be narrowly tailored and will not discriminate based on viewpoint.
- D. 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, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.

- F. The use of a "Proxy" server or service to bypass the filtering technology is not allowed and is a violation of this policy. Defeating or bypassing the filtering technology is also a violation of CIPA (Children's Internet Protection Act, [Federal Act, 2000]).

VIII. CONSISTENCY WITH OTHER SCHOOL POLICIES

All use of electronic technology must be consistent with School District policies and the mission of the School District.

IX. NO REASONABLE EXPECTATION OF PRIVACY

- A. By authorizing use of Electronic Technology, the School District does not relinquish exclusive control over its Electronic Technology or any data accessed, reviewed, uploaded, downloaded, stored, maintained, printed, posted, transmitted, or distributed using Electronic Technology. Users have no reasonable expectation of privacy in the contents of any data, including personal files that are accessed, reviewed, uploaded, downloaded, stored, maintained, printed, posted, transmitted, or distributed using Electronic Technology.
- B. The School District retains full ownership, authority, and control over its Electronic Technology. To the full extent permitted by law, the School District may monitor and inspect the use of Electronic Technology, including, but not limited to, any data that are accessed, reviewed, uploaded, downloaded, stored, maintained, printed, posted, transmitted, or distributed using Electronic Technology. Such monitoring and inspection may occur as authorized by the Superintendent, or the Superintendent's designee, without any notice to the user.
- C. Routine maintenance, monitoring, or inspection of Electronic Technology may lead to a discovery that a user has violated this policy, another School District policy, or the law.
- D. An investigation or search related to employee use will be conducted when authorized by the Superintendent, the Superintendent's designee, or the School Board. An investigation or search related to student use will be conducted when authorized by the building principal or assistant principal, the Superintendent, the Superintendent's designee, or the School Board.
- E. 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.
- F. 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.
- G. 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.
- H. Parents and guardians should notify the building principal if they have concerns about their child's access to or use of Electronic Technology.
- I. School District employees should be aware that data and other materials in files that are sent, received, or maintained on or through the use of Electronic Technology are subject to review, disclosure, or discovery under Minnesota Statutes, Chapter 13 (the Minnesota Government Data Practices Act).
- J. Subject to the Minnesota Government Data Practices Act, 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.

X. 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/guardians, and employees of the School District.
- B. Before using Electronic Technology to access the Internet, students and School District employees are required to review and sign an Internet Use Agreement.
- C. In lieu of the Internet Use Agreement Form, the District may use a pop-up window requiring students and employees to accept the terms and conditions as stated in the Internet Use Agreement before access will be granted to the user.

XI. LIMITATION ON SCHOOL DISTRICT LIABILITY

All use of Electronic Technology is at the user's own risk. Electronic Technology is provided on an "as is, as available" basis. The School District is not responsible for any damage users may suffer, including, but not limited to, loss, damage or unavailability of data accessed, processed, or stored on any Electronic Technology; for delays or changes in or interruptions of service; or any delivery or non-delivery 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 Electronic Technology. The School District will not be responsible for financial obligations arising through unauthorized use of Electronic Technology.

XII. USER NOTIFICATION

- A. All users will be notified of this Policy. This notification will include the following:
 - 1. Notification that Electronic Technology use is subject to compliance with School District policies.
 - 2. Disclaimers limiting the School District's liability relative to the use of Electronic Technology.
 - A. Information stored on school district diskettes, hard drives, or server.
 - B. Information retrieved through school district computers, networks, or online resources,
 - C. Personal property used to access district computers, networks, or online resources.
 - D. Unauthorized financial obligations resulting from use of school district resources/account to access the Internet.
 - 3. A description of the private rights and limitations of school sponsored/managed Internet accounts.
 - 4. Notification that, even though the School District may use technical means to limit student Internet access, these limits do not provide a foolproof means for enforcing the provisions of this acceptable use policy.
 - 5. Notification that goods and services can be purchased over the Internet that could potentially result in unwanted financial obligations and that any financial obligation incurred by a student through the Internet is the sole responsibility of the student and/or the student's parents/guardians.
 - 6. Notification that the collection, creation, reception, maintenance, and dissemination of data via the Internet, including electronic communications, is governed by Policy 406, Public and Private Personnel Data, and Policy 515, Protection and Privacy of Pupil Records.

7. Notification that, should the user violate the School District's acceptable use policy, the user's access privileges may be revoked, school disciplinary action may be taken and/or appropriate legal action may be taken.
8. Notification that all provisions of the acceptable use policy are subordinate to local, state, and federal laws.

XIII. PARENTS' 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 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.

XIV. 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.