

RICHFIELD PUBLIC SCHOOLS

ELECTRONIC USE AND COMMUNICATIONS

I. PURPOSE

The purpose of this policy is to set forth guidelines for access to and appropriate use of the Richfield Public School District's digital technologies and wireless and wired computer network systems. This includes, but is not limited to, acceptable and safe use of District-provided devices for student academic use.

II. GENERAL STATEMENT OF POLICY

In making decisions regarding employee and student access to the District's digital technologies, wireless and wired computer network systems, and software applications, including electronic communications, the District considers its own stated educational mission, goals, and objectives -- digital literacy, fluency, and citizenship, along with electronic information research skills are fundamental to the preparation of citizens and future employees. Access to the District's computer systems and to the internet enables students and employees to explore thousands of resources while communicating and collaborating with people around the world. The school district expects that all users will blend thoughtful use of the District's computer system and the internet throughout curriculum and instruction and will provide guidance to students in their use.

III. DEFINITIONS

- A. Communications equipment and networks: includes, but is not limited to, telephones (VoIP), voicemail, fax machines, desktop and laptop computers, Chromebooks, tablets, computer networks, email, and the internet.
- B. Electronic communications: The sharing of information and ideas through the use of electronic communications devices and internet applications. Electronic communications may have a permanency like that of paper communication and may be traceable to the sender. Applicable modes of communication include, but are not limited to, telephone/cell phone, voicemail, fax transmissions, computers, software, phone and computer applications, operating systems, computer networks, email, storage media, file transfer protocol (FTP), portable electronic devices, social media, and the internet.
- C. Intellectual property: An individual's own thoughts and ideas expressed through a product such as a drawing or written document which may

be viewed in the form of a tangible, "hard copy" such as paper or stored electronically and viewed on a monitor or screen. Student homework and teacher-created curricular items are specific examples.

D. Internet: A world-wide network of computers. Internet access is viewed both as an extension of the District's email and as an extension of the schools' digital resources. This includes email, the World Wide Web, social media, streaming media, and other similar electronic content.

E. Copyright: The exclusive right granted by the federal government to reproduce, publish, and sell the matter and form of a literary, musical, or artistic work. Permission must be received from copyright holders before copyrighted works can be used by others.

F. Fair use: A copyright law doctrine which permits educational organizations and staff rights to legal, non-licensed citation or incorporation of copyrighted materials within the confines of the educational environment for criticism, comment, and instructional purposes.

G. Eligible students: All rights and protections given parents/guardians under this policy transfer to the student when the student reaches eighteen (18) years of age or enrolls in an institution of post-secondary education. The student then becomes an "eligible student." However, the parents/guardians of an eligible student who is also a "dependent student" are entitled to gain access to the educational records of such student without first obtaining the consent of the student.

H. Access: Refers to a staff or student's rights to hardware and software provided by Richfield Public Schools. Access can be altered or even denied if a user violates this or other Board Policies.

I. Bullying: Refer to Board Policy 113 (Bullying Prohibition Policy)

IV. LIMITED EDUCATIONAL PURPOSE

The District is providing students and employees with access to the District's digital network system, hardware, and software, which includes internet access. The purpose of the District's digital network system is more specific than providing students and employees with general access to the internet. District communication systems and resources have limited educational purposes, which include the use of the resources and system for classroom activities, educational research, and professional or career development. Users are expected to use access through the District's digital network resources and system to further educational and personal goals consistent with the mission of the school district and school policies. Uses which might be acceptable to a user's private personal account or equipment on another system may not be acceptable on this limited-purpose system.

V. PROHIBITED USES

- A. While not an exhaustive list, the following uses of the District's system, hardware, software, and internet resources or accounts are considered unacceptable:
1. Users will not use the District's 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's 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 District's system to engage in any illegal act or violate any local, state, or federal statute or law.
 4. Users will not use the District's 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's system software, hardware, or wiring or take any action to violate the District's security system, and will not use the District's system in such a way as to disrupt the use of the system by other users.

5. Users will not use the District's 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's 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, unapproved 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 the District's website 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 digital presences 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 District's as directory information and verification is made that the 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 581; or
 - (2) Such information is not classified by the 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 581.

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 or the District's Director of Marketing & Communications.

- 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, "Facebook, X, formerly known as Twitter, Instagram, Snapchat, TikTok, etc."

7. Users will not attempt to gain unauthorized access to the District's system or any other system through the District's 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's system may not be encrypted without the permission of appropriate school authorities.
8. Users will not use the District's 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 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 District's 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's system to offer or provide goods or services or for product advertisement, except for in the case of school-related fundraisers.
10. Users will not use the District's system to engage in bullying or cyberbullying in violation of the District's Bullying Prohibition Policy 113. 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. The District has a special interest in regulating off-campus speech that materially disrupts classwork or involves substantial disorder or invasion of the rights of others. A student or employee engaging in unacceptable use of the internet when off 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, serious or severe bullying or harassment targeting particular individuals; threats aimed at teachers or other students; failure to follow rules concerning lessons, the writing of papers, the use of

computers, or participation in other online school activities; and breaches of school security devices. If the District receives a report of an unacceptable use originating from a non-school computer or resource, the 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 District computer system and the internet and discipline 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 a 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 District employee, the building administrator.

VI. LIMITATIONS ON SCHOOL DISTRICT LIABILITY

Use of the District's 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, cloud services, or servers (physical or virtual), 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 school district system. The District will not be responsible for financial obligations arising through unauthorized use of the school district system or the internet.

VII. INTERNET SAFETY

The District will employ technical systems designed to restrict and monitor access to materials harmful to minors, including but not limited to internet filtering systems. Access to systems such as email and social media will be limited to curriculum-related work only.

- 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.
 - 2.
 - 3.
 - 4.
 - 5.
 - 6.
 - 7.
 - 8.
 - 9.
 - 10.
 - 11.
 - 12.
 - 13.
 - 14.
 - 15.
 - 16.
 - 17.
 - 18.
 - 19.
 - 20.
 - 21.
 - 22.
 - 23.
 - 24.
 - 25.
 - 26.
 - 27.
 - 28.
 - 29.
 - 30.
 - 31.
 - 32.
 - 33.
 - 34.
 - 35.
 - 36.
 - 37.
 - 38.
 - 39.
 - 40.
 - 41.
 - 42.
 - 43.
 - 44.
 - 45.
 - 46.
1. Obscene;
 2. Child pornography;
 3. Harmful to minors; or
 4. Detrimental to, or obstructive of a student's ability to learn in a safe, productive environment.
- 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 District will educate students about appropriate online behavior, including interacting with other individuals on social networking websites and will actively train students on digital fluency, literacy, and cyberbullying awareness and response.

VIII. PRIVACY EXPECTATIONS

- A. The District maintains control of the materials on its systems contained in files on the system. Users should not expect privacy in the contents of personal files on the District's systems. Files stored on District computers and servers should not be considered the private property of individuals and may be viewed by supervisory school employees.

- B. Routine maintenance and monitoring of District systems 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. In accordance with the Minnesota Student Data Privacy Act (Minn. Stat. 13.32), the District does not regularly nor routinely track student activity in digital environments, unless alerted to a concern of student harm or imminent threat. In such cases, students and/or their families are notified within 72 hours of the alert.
- D. Parents/guardians may have the right at any time to investigate or review the contents of their child's files and email files by way of written request in accordance with Policy: 581: Protection and Privacy of Pupil Records.
- E. District employees 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, 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 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's systems.

IX. USER NOTIFICATION

- A. All users shall be notified of the District's policies relating to the use of the District's digital network system and internet use.
- B. This notification shall include the following:
 - 1. Notification that use of the District's digital network system and internet use is subject to compliance with District policies.
 - 2. Disclaimers limiting the District's liability relative to:
 - a. Information stored on District hard drives, cloud-based storage, or servers.
 - b. Information retrieved through 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 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 District may use technical means to limit student and staff internet access, these limits do not provide a foolproof means for enforcing the provisions of this responsible 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 412: Public and Private Personnel Data, and Policy 581: Protection and Privacy of Pupil Records.
 7. Notification that, should the user violate the District's responsible 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 responsible use policy are subordinate to local, state, and federal laws.

X. PARENT/GUARDIAN RESPONSIBILITY; NOTIFICATION OF STUDENT INTERNET USE

- A. Outside of school, parents/guardians bear responsibility for the same guidance of internet use as they exercise with information sources such as television, telephones, smartphones, tablets, personal computers, radio, movies, streaming content, video games, and other possibly offensive media. Parents/guardians are responsible for monitoring their child's use of the District's system and of the internet if the child is accessing the District's system from home or a remote location.

B. Parents/guardians will be notified that their child will be using District resources/accounts to access the internet. 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 statement that the Internet Use Agreement must be digitally or physically signed by the user and the parent or guardian prior to use by the student.
4. A statement that the District's responsible use policy is available for parental review on the District website.

XIII. ARTIFICIAL INTELLIGENCE (AI)

A. The use of Artificial Intelligence (AI) tools is common in educational settings and is a rapidly evolving area of interest. We encourage students to take advantage of these tools responsibly to enhance their learning experience. However, it's important to remember the following guidelines:

1. **AI-Assisted Original Work:** While students are encouraged to utilize AI tools for studying, homework, and researching, any work submitted must reflect the student's own understanding and knowledge. Students should not use AI-generated content as their own without appropriate understanding and processing of the information. This includes AI-created essays, solutions to problems, or any other assignments that are not the result of the student's own intellectual efforts.
2. **Responsible Use of AI:** Students should not allow other students to copy or use their original work that has been AI-assisted. Sharing AI-generated answers or enabling others to pass off AI-assisted work as solely their own is against District policy.
3. **AI and Plagiarism:** Just as copying information from websites or other resources without giving proper credit is plagiarism, using AI-generated content without due acknowledgment or understanding is also a form of plagiarism. Students should not represent AI-generated content as their own original work. Instead, students are allowed and encouraged to use AI tools to help them in the academic process, not as a substitute for their own authentic work.

B. Cases involving academic dishonesty, including misuse of AI, may be handled by the classroom teacher or may be referred to the

administration. Consequences may include, but are not limited to: an assignment being reset, consultation with the media center staff on appropriate and inappropriate uses of AI before any more assignments may be attempted, additional monitoring of student work, limitation of devices and digital resource access.

C. We trust in our students' ability to use AI tools responsibly, with the goal of enhancing their learning experience rather than compromising the integrity of their work. As the District works to codify an aligned policy around Artificial Intelligence usage, students and staff agree to the following conditions as violations of acceptable conduct:

1. Creation or distribution of false or misleading content.
2. Impersonation of others
3. Manipulation of academic or personal records.
4. Sharing or exposing any personally identifiable information (PII), including student, staff, or District information, to individuals who do not have explicit authorization or the necessary permissions to access such data.
5. Producing or submitting work that is not their own, including copying content without proper attribution or presenting AI-generated content as original work.

XIV. IMPLEMENTATION; POLICY REVIEW

- A. The District administrators 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/guardian notifications, if necessary, to reflect the adoption of these guidelines and procedures.
- C. The District's internet policies and procedures are available for review by all parents, guardians, staff, and members of the community on the District website.
- 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:

1
2 Minn. Stat. Ch. 13 (Minnesota Government Data Practices Act)
3 15 U.S.C. § 6501 *et seq.* (Children's Online Privacy Protection Act)
4 17 U.S.C. § 101 *et seq.* (Copyrights)
5 20 U.S.C. § 1232g (Family Educational Rights and Privacy Act)
6 47 U.S.C. § 254 (Children's Internet Protection Act of 2000 (CIPA))
7 47 C.F.R. § 54.520 (FCC rules implementing CIPA)
8 Minn. Stat. § 121A.031 (School Student Bullying Policy)
9 Minn. Stat. § 125B.15 (Internet Access for Students)
10 Minn. Stat. § 125B.26 (Telecommunications/Internet Access Equity Act)
11 *Mahanoy Area Sch. Dist. v. B.L.*, 594 U.S., 141 S. Ct. 2038 (2021)
12 *Tinker v. Des Moines Indep. Cmty. Sch. Dist.*, 393 U.S. 503 (1969)
13 *United States v. Amer. Library Assoc.*, 539 U.S. 1942003)
14 *Sagehorn v. Indep. Sch. Dist. No. 728*, 122 F.Supp.2d 842 (D. Minn. 2015)
15 *R.S. v. Minnewaska Area Sch. Dist. No. 2149*, 894 F.Supp.2d 1128 (D. Minn. 2012)
16 *Tatro v. Univ. of Minnesota*, 800 N.W.2d 811 (Minn. App. 2011), *aff'd* on other
17 grounds 816 N.W.2d 509 (Minn. 2012)
18 *S.J.W. v. Lee's Summit R-7 Sch. Dist.*, 696 F.3d 771 (8th Cir. 2012)
19 *Parents, Families and Friends of Lesbians and Gays, Inc. v. Camdenton R-III Sch.*
20 *Dist.*, 853 F.Supp.2d 888 (W.D. Mo. 2012)
21 *M.T. v. Cent. York Sch. Dist.*, 937 A.2d 538 (Pa. Commw. Ct. 2007)
22
23

24 **Cross References:**

25 Board Policy 103: Harassment Prohibition
26 Board Policy 109: Distribution of Materials on School Premises
27 Board Policy 113: Bullying Prohibition
28 Board Policy 412: Public and Private Personal Data
29 Board Policy 452: Evaluation and Development of Professional Staff
30 Board Policy 541: Student Behavior
31 Board Policy 581: Protection and Privacy of Pupil Records
32 Board Policy 601: Academic Standards and Instructional Curriculum
33 Board Policy 607: Online Learning Options
34 Board Policy 608: Education of Students with Disabilities
35 Board Policy 610: Selection and Reevaluation of Instructional Material
36 Board Policy 611: Provision for Alternative Instruction
37 Board Policy 612: Curriculum Development
38 Board Policy 616: School Sponsored Student Publications
39 Board Policy 802: Crisis Management
40 Employee handbooks, collective bargaining agreements
41
42

43 RATIFIED BY THE BOARD OF EDUCATION: September 16, 1996
44

45 REVISED BY THE BOARD OF EDUCATION: August 23, 1999; October 15, 2001;
46 November 20, 2006; December 4, 2007; March 16, 2015; April 19, 2021; September
47 6, 2022; September 16, 2024; August 17, 2026
48

- 1 REVIEWED AND REAFFIRMED BY THE BOARD OF EDUCATION: February 5,
- 2 2001; August 16, 2021; September 5, 2023; August 18, 2025