

**RICHFIELD PUBLIC SCHOOLS**

**ADMINISTRATIVE GUIDELINES**

**ELECTRONIC USE AND COMMUNICATIONS**

Richfield Public Schools' technology and communication resources are intended for authorized users only. The purpose of these administrative guidelines is to assist in the implementation of Board Policy 107 pertaining to the appropriate usage of these resources.

Inappropriate use exposes Richfield Public Schools to risks including virus attacks, compromise of network systems and services, and legal issues. It is the responsibility of every technology resources user to know these guidelines and to conduct their activities accordingly.

**A. NOTIFICATION**

1. The school principal shall develop and distribute site-specific information, which is aligned with these guidelines.
2. Relevant parts of these guidelines shall be distributed to all staff, students, and parents/guardians. They shall also be posted in media centers, computer labs, and flexible learning spaces.

**B. DEFINITIONS**

1. **AUTHORIZED USER** – Employees or students of the Richfield Public Schools, or visitors specifically authorized by the District.
2. **AUTHORIZED USES** – All staff are authorized to use technology resources for administration, curriculum development, student instruction, personal productivity and professional development. Students are authorized to use technology resources for school-based programs and activities. Authorized visitors are able to utilize technology resources for school-based programs, school-based activities, or District approved activities.
3. **TRAINING** – Development opportunities include online, district provided, externally provided, on site and off site instruction.

**C. TRAINING**

1. **TECHNOLOGY STANDARDS** – Technology standards shall be periodically updated to include relevant technology expectations for staff. Staff shall have access to training related to professional expectations.

- 1           2.    NEW STAFF – The Director of Technology shall coordinate plans to  
2           insure that training is provided for all new staff on network access, network  
3           accounts, email accounts, passwords and required information systems.  
4           This training shall generally be coordinated and delivered by the District's  
5           digital learning coach, technology lead teachers, and media specialists.  
6
- 7           3.    STUDENT INSTRUCTION – As part of the instructional program, all  
8           students will receive instruction on the following as appropriate:  
9
  - 10           •   responsibilities, privacy, and acceptable usage of systems
  - 11
  - 12           •   web information tools and appropriate search techniques so students  
13           will be able to use the internet in an efficient manner
  - 14
  - 15           •   login and password use for network accounts and email
  - 16
  - 17           •   accessing grade and attendance information from online systems  
18           utilized by the District
  - 19

20 **D.    SETUP AND USE OF COMPUTERS AND THE NETWORK**

- 21
- 22           1.    PLATFORM –Use of software platforms and hardware will be limited to  
23           those creating specific teaching, learning, and school management  
24           benefits.  
25
- 26           2.    ACCESS CONTROL – All computers or devices connecting to District  
27           technology resources shall have access control that restricts the use to  
28           authorized persons.  
29
- 30           3.    CRITICAL AREAS – Critical technology equipment including, but not  
31           limited to, telephone cabinets, , switches, servers and wiring racks shall be  
32           kept in locked areas. This equipment shall include uninterrupted power  
33           supplies, surge protection, and environmental controls for temperature  
34           and humidity where applicable.  
35
- 36           4.    STANDARD CONFIGURATION – Hardware and software will be  
37           configured by vendors and/or technology support personnel in a known  
38           and documented manner that can be easily restored if necessary.  
39
- 40           5.    NETWORK RESOURCES – Use of the school network shall be in a  
41           manner as to conserve the resources of the network. This includes traffic  
42           generated on the network, as well as files saved on servers. Individuals  
43           are expected to remove old and unnecessary files from network storage.  
44           Student files will be deleted 30 days after the end of each school year.  
45
- 46           6.    PRINTING LOCATIONS – Printers shall be strategically located for ease  
47           of use and to reduce maintenance and hardware costs. Document  
48           printing centers shall be the primary location to print documents in excess

1 of 10 pages. These locations will be determined by building  
2 administrators.

3  
4 7. SCANNING FOR VIRUSES – Virus scanning software shall be installed  
5 on all school issued computers with virus definition files kept up-to-date.  
6 Non-school issued computers will be restricted to use on a network that is  
7 separate from the internal network unless specifically authorized by the  
8 Director of Technology or authorized representative of the technology  
9 department.

10  
11 8. INTERNET AND EMAIL FILTERING – Redundant systems shall be  
12 installed to block inappropriate internet sites and email messages. This  
13 system shall allow the addition or removal of individual internet sites and  
14 email addresses from a list of those to be blocked. Staff may submit  
15 requests for changes to the blocking list to the Director of Technology for  
16 consideration by a committee made up of instructional representatives, the  
17 Director of Technology, and a member of the technology department.

18  
19 9. RESPONSIBILITY FOR INTERNET USE – Each individual has the  
20 responsibility to avoid inappropriate sites, and to report any occurrence of  
21 inappropriate internet use to building staff or administration. Although  
22 systems to block access to inappropriate internet sites are in place, it is  
23 not possible to block all sites that may contain inappropriate or  
24 undesirable material. If a user inadvertently accesses unacceptable  
25 materials or an unacceptable internet site, the user shall immediately  
26 disclose the inadvertent access to an appropriate District official. In the  
27 case of an employee, the immediate disclosure shall be to the employee's  
28 immediate supervisor and/or the building administrator. This disclosure  
29 may serve as a defense against an allegation that the user has  
30 intentionally violated this policy.

31  
32 10. REFORMAT COMPUTERS- District computers will be reconfigured when  
33 an employee leaves the District or a computer is reassigned. Files or  
34 individual applications may be removed. It is the responsibility of the  
35 individual to back up their files before returning their computer for reuse.

36  
37 **E. STAFF, STUDENT AND TENANT NETWORK ACCESS AND ACCOUNTS**

38  
39 TECHNOLOGY SUPPORT PROVIDER – The District Technology Support Team  
40 shall support network accounts, network resources, passwords and  
41 software/hardware maintenance. Building staff shall report all technology  
42 support requests to the technology support provider via the District help desk  
43 system. District technology support staff shall initiate or coordinate basic repairs  
44 on equipment and/or coordinate requests for repair or network services in a  
45 timely manner.

46  
47 1. DISTRICT ACCOUNTS – User accounts shall be setup as follows:  
48

- 1                   • Each user shall be authorized to use the adequate features necessary  
2                   rather than all available features possible.
- 3
- 4                   • Accounts shall be accessible via an intranet portal for access in and  
5                   away from school.
- 6
- 7                   • Students no longer enrolled in Richfield Public Schools will have  
8                   limited account access upon leaving the District, and their accounts  
9                   permanently removed 30 days after being unenrolled or on June 30 of  
10                  the school year they are last enrolled, whichever occurs first.
- 11
- 12                  • Staff no longer employed in Richfield Public Schools will have limited  
13                  account access upon ending employment with the District either  
14                  voluntarily or involuntarily, and their accounts permanently removed 30  
15                  days after ending employment or on June 30<sup>th</sup> of the school year they  
16                  are last employed, whichever occurs first.
- 17
- 18                  2.    TENANTS' ACCOUNTS – Tenants and other non-authorized users of  
19                  District facilities desiring access to the network must follow District  
20                  operating procedures in obtaining and maintaining network access and  
21                  accounts.
- 22
- 23                  3.    LOG OFF – Employees should log out of accounts when finished with  
24                  their use. Computers should be turned off at the end of the day, unless  
25                  specifically requested to leave them on. Logged on computers should  
26                  never be left unattended at workstations.
- 27
- 28                  4.    PASSWORDS – Staff and students are expected to use passwords and  
29                  keep them secure. Automated systems shall periodically expire  
30                  passwords, yet notify users that passwords are about to expire.  
31                  Individuals are expected to respect the privacy and security of others.  
32                  Persons should not watch when others are entering their password.  
33                  Users should not write passwords where others may access them and  
34                  should change a password as soon as possible if they suspect someone  
35                  else knows it. New password creation and management structures such  
36                  as multi factor authentication (MFA) may be forced at any time by the  
37                  District technology department with a 30 day prior notice to affected users.
- 38
- 39                  5.    PERSONAL BACKUPS – Storage will be available on District computers  
40                  or servers to support the instructional activities of staff and students. All  
41                  individuals are encouraged to make backups of their important work, since  
42                  files on District computers and cloud-based systems cannot be  
43                  guaranteed.
- 44
- 45                  6.    UNAUTHORIZED USE OR ACCESS REVOKING ACCOUNTS –  
46                  Depending on the nature and degree of the violation and the number of  
47                  previous violations, unacceptable use of the District's system or the  
48                  internet may result in one or more of the following consequences:

1 suspension or cancellation of use or access privileges; payments for  
2 damages and repairs; discipline under other applicable District policies,  
3 including suspension, expulsion, exclusion or termination of employment;  
4 or civil or criminal liability under other applicable laws.  
5

6 Unauthorized access could include but is not limited to network and email  
7 accounts, network administrative functions, computer lab management  
8 software, unauthorized internet sites, infrastructure resources, printers,  
9 servers, switches, and networking closets.  
10

11 If unauthorized uses are observed or documented, the following actions  
12 may be taken:  
13

- 14 • Staff: temporary suspension of an account by an administrator or  
15 designee in accordance with provisions of employee contracts.  
16
- 17 • Students: network and email privileges may be temporarily suspended  
18 by a supervising staff member, or suspended for a period of time not to  
19 exceed one (1) school year by building administration according to the  
20 school's discipline policies.  
21

#### 22 7. INTERNET USE AGREEMENT AND DISCLAIMER

23 The proper use of the internet and the educational value to be gained from  
24 proper internet use is the joint responsibility of students,  
25 parents/guardians, and employees of the District.  
26

- 27 • An Internet Use Agreement form for students must be read and  
28 physically or digitally signed by the user and the parent or guardian.  
29 The Internet Use Agreement form for employees must be signed by  
30 the employee and filed at the District office, physically or virtually.  
31
- 32 • All users shall be notified of the District policies relating to internet  
33 use. Notification shall include:
  - 34 ○ Disclaimers limiting the District's liability
  - 35 ○ A description of privacy rights and limitations
  - 36 ○ Notification that means used to limit student access do not provide  
37 a fool proof means for enforcing provisions of this policy
  - 38 ○ Notification that violation of the acceptable use policy may result in  
39 revocation of privileges, school disciplinary action or other  
40 appropriate legal action  
41

- 42 8. PARENT/GUARDIAN OPT OUT OF STUDENT INTERNET USE –  
43 Parents/guardians may request alternative activities for their children that  
44 do not require internet access or computer use. If parents/guardians  
45 exercise this right, the students will have no internet or computer access  
46 throughout the District.  
47

#### 48 F. SOFTWARE

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  
47

1. LEGAL LICENSING – The District will install and use only legally purchased and licensed software on District computers and servers. The District will purchase software licenses for each computer, site licenses or concurrent use licenses.
2. CURRENT SUPPORTED SOFTWARE – Curriculum software shall be aligned with academic standards and curricular needs based on teacher recommendation and shall be approved by the District teaching and learning staff and the District network staff prior to purchase.
3. INSTALLATION OF DISTRICT-WIDE SOFTWARE – Technology support staff shall load operating system software, District-wide application software, local application software, or peripherals onto District computers or onto district servers.
4. SYSTEM SOFTWARE – System software shall be maintained as the vendor has intended, unless modification is recommended by the District technical staff and approved by District administration.
5. COPYING APPLICATIONS – A software application shall not be copied to another computer without a legal license or procedure to pay for that additional license.
6. HOME SOFTWARE – Use of software applications (purchased for home use by staff or students) on school computers is prohibited. Use of school applications on home computers is prohibited, unless specifically allowed in the software license.

**G. ADDING EQUIPMENT BY PURCHASE OR DONATION**

1. NETWORK ACCESSIBILITY – Technology equipment purchased or obtained for use by students, teachers, administrators, and/or staff with the capability of fully utilizing network and internet resources, will be considered for both the intended use at the time of purchase and future, undetermined uses.
2. CONSIDERATIONS FOR ADDITIONAL EQUIPMENT – Criteria for identifying computer and network hardware for purchase, or for accepting donated hardware, will include:
  - The alignment of the computer hardware to educational outcomes for students and teachers.
  - The educational and developmental appropriateness of the hardware.

- 1                   ▪ The ability of technical support staff to administer and maintain the
- 2                   equipment.
- 3
- 4                   ▪ The ability to operate and communicate with the existing network
- 5                   configuration in place or being developed at the time of acquisition.
- 6
- 7                   ▪ The ability of the District to maintain low total cost of ownership (TCO),
- 8                   to include initial purchase cost, ongoing maintenance costs, costs for
- 9                   necessary and/or desired software, and purchase of replacement
- 10                  parts.

11

12           3.    **APPROVAL PROCEDURES** – All purchases of instructional and non-

13           instructional software, computer, and video and media hardware must be

14           approved by the Director of Technology before being placed in the

15           District’s order entry system. The Director of Technology will also approve

16           re-installation of previously removed software after verification that such

17           software aligns with current curriculum and student objectives, as well as

18           wider District strategic goals.

19

20           All purchases of network infrastructure hardware and software must be

21           approved by the District’s technology support department before being

22           placed in the District’s order entry system.

23

24           All potential donations of computer technology or equipment must be

25           approved by the Director of Technology and Director of Finance before

26           being accepted and added to the District equipment inventory system.

27           Technology support personnel shall assist in the evaluation of donated

28           equipment prior to its acceptance by the District.

29

30           4.    **TECHNOLOGY SPECIFICATIONS** – Technology specifications shall be

31           developed and updated at appropriate intervals to reflect current software

32           and workstation requirements for new and donated equipment.

33

34   **H.    HOME USE OF COMPUTERS**

35

36           1.    **AUTHORIZED USERS** – Current employees and students of the District

37           may, upon completion of proper forms or procedures as developed, use

38           school computer, technology and/or electronics equipment at their home

39           for school use.

40

41           2.    **APPROVAL PROCEDURES** – Procedures for the sign-out of school

42           equipment shall be developed by the District’s technology department and

43           maintained by the building administration or designee. Signatures will be

44           obtained from the appropriate building administrator, building media

45           specialist or technology support provider, and the employee or student

46           making the request. Procedures and criteria for approving the request will

47           include completion of a request form that addresses all personal care and

1 responsibility guidelines listed under H.3 of these administrative  
2 guidelines.

3  
4 **3. PERSONAL CARE AND RESPONSIBILITY**

- 5
- 6 ■ Building administrators or designee will record the dates when  
7 equipment may be taken off the school property and the deadline date  
8 by which equipment should be returned.
  - 9
  - 10 ■ Equipment should be in nearly the same working order when returned  
11 as when signed out.
  - 12
  - 13 ■ No unauthorized changes or additions will be made to the equipment.
  - 14
  - 15 ■ The District is not liable for any damages to personal property that may  
16 result from the use of school equipment by the user outside the schools.
  - 17
  - 18 ■ The user is potentially liable for repair or replacement costs, which may  
19 arise due to damage or loss of the equipment. Such costs will be  
20 clearly defined on user signed documentation collected as part of the  
21 checkout process.
  - 22

23 **I. USE OF PERSONAL DIGITAL DEVICES AT SCHOOL WORKSITES**

- 24
- 25 1. **AUTHORIZED USERS** – Current employees, students, and authorized  
26 visitors of the Richfield Public Schools may, with prior approval, use their  
27 personal digital devices for school related tasks on the District's guest  
28 network.
  - 29
  - 30 2. **INSTALLATION, MAINTENANCE AND REMOVAL**
  - 31
  - 32 ■ The date when equipment is added to the District network will be  
33 recorded.
  - 34
  - 35 ■ Personal computers or digital devices shall not be repaired,  
36 maintained, nor have other hardware changes or additions provided by  
37 District staff.
  - 38
  - 39 ■ The District is not liable for any damages or loss (including theft) to  
40 personal property that may result from the use of personal equipment  
41 at the school work site.
  - 42

43 **J. STAFF USE OF EMAIL, VOICEMAIL, PHONE AND FAX**

- 44
- 45 1. **ETIQUETTE** – Individuals sending messages using District technology  
46 such as voicemail and email should keep in mind that they are perceived  
47 as a representative of the Richfield Public Schools.
  - 48



- 1           2.     **VOICE MESSAGES**– Voicemail messages are not backed up or archived  
2                    by network personnel. Messages are automatically deleted after 90 days.  
3
- 4           3.     **STAFF EMAIL**- Staff email is archived for a period of three (3) years from  
5                    the date the message was sent or received.  
6
- 7           4.     **STUDENT EMAIL**- Student email, sent or received, is archived for a  
8                    period of one (1) year from the date the message was sent or received, or  
9                    upon removal of the account, whichever comes first.  
10
- 11          5.     **MESSAGES ARE NOT PRIVATE** – Messages stored on District systems  
12                    or District authorized systems shall not be considered private property and  
13                    may be accessed by District administrative employees. This would  
14                    generally be done to resolve technical problems or at the request of  
15                    administration.  
16
- 17          6.     **CONSERVE RESOURCES** – Individuals should use the voicemail, email  
18                    and fax systems in a manner to conserve resources  
19
- 20          7.     **AVOID AUTOMATIC FORWARDING** – Emails sent to District email  
21                    addresses should not be setup to automatically forward to external email  
22                    locations in order to avoid the distribution of sensitive student or employee  
23                    information.  
24
- 25          8.     **900 NUMBERS** – Calls to 900 numbers shall not be permitted.  
26

27 **K.     WEBSITE MANAGEMENT**

- 28
- 29          1.     **WEBSITES** – Schools and District programs shall have the opportunity to  
30                    post content on the official school and District websites to enhance  
31                    communication with students, families, and the community. These  
32                    websites were established within systems agreed upon by the Director of  
33                    Marketing & Communications, the Technology Director, and the District  
34                    Technology Advisory Committee (DTAC).  
35
- 36            a.     **Intranet:** An internal “intranet” website will be maintained for uses  
37                    specific to internal Richfield Public Schools authorized users.  
38                    Technical management of the intranet will be done by the  
39                    communications department and the technology department. Content  
40                    for the site will be determined by District administration. Teachers,  
41                    building staff, and building administration may provide  
42                    recommendations for additional site content.  
43
- 44          2.     **WEBSITE PUBLISHING RIGHTS** – The Director of Marketing &  
45                    Communications and the Director of Technology have the responsibility  
46                    for granting publishing rights to District or school websites. These rights  
47                    may be extended to employees, students, parents/guardians and/or  
48                    community members. Training shall be provided to all users prior to

1 granting of publishing rights to ensure effective use of the system, and to  
2 emphasize proper etiquette and accepted format to professionally and  
3 appropriately represent Richfield Public Schools. Training includes, but is  
4 not limited to, ADA compliance in web content, AP Style, and District  
5 brand guidelines. Employees should not create public, school-related  
6 websites outside of the official school or District websites. Teachers  
7 should use school-approved learning management systems for  
8 communicating with students and families. If educators or other District  
9 staff create Google sites for communication purposes, they should be set  
10 to be visible only to District students and staff; they should not be public.

11  
12 3. WEBSITE CONTENT EXPECTATIONS – Teaching staff, program  
13 leaders, and administrators are expected to provide up-to-date website  
14 content with information of interest to District staff, students and the  
15 community. Expectations shall be developed by the Director of Marketing  
16 & Communications and district administration, monitored at the building  
17 level by building administration.

18  
19 4. STUDENT WEBSITES – Student websites will not be provided through  
20 the District website structure. However, students may occupy web  
21 presences such as blogs, Google Sites, etc. Training shall be provided to  
22 students prior to granting publishing rights to ensure effective use of the  
23 systems, and to emphasize proper etiquette and industry accepted  
24 formats, which appropriately represent Richfield Public Schools. Sites that  
25 contain inappropriate content, inaccurate information, or are not a positive  
26 representation of Richfield Public Schools will be edited or removed,  
27 generally at the recommendation of the Director of Marketing &  
28 Communications and the appropriate building or District administrator.

29  
30  
31 Dated: February 5, 2001

32  
33 Reviewed: November 4, 2007; April 6, 2015; August 16, 2021

34  
35 Revised: November 20, 2006; April 19, 2021  
36