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 ransomware, virus attacks, compromise of network systems and services, and legal issues. It is the responsibility of every technology resource user to know these guidelines and to conduct their activities accordingly.

A. NOTIFICATION

1. The director of technology shall coordinate with the school principals to 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 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.

2. NEW STAFF – The director of technology shall coordinate plans to ensure that training is provided for all new staff on network access, network accounts, email accounts, passwords and required information systems. This training shall generally be coordinated and delivered by the District's digital learning coach, technology lead teachers, and media specialists.

3. STUDENT INSTRUCTION – As part of the instructional program, all students will receive instruction on the following as appropriate:

- responsibilities, privacy, and acceptable usage of systems
- web information tools and appropriate search techniques so students will be able to use the internet in an efficient manner
- login and password use for network accounts and email
- accessing grade and attendance information from online systems utilized by the District

D. SETUP AND USE OF COMPUTERS AND THE NETWORK

1. PLATFORM – Use of software platforms and hardware will be limited to those creating specific teaching, learning, and school management benefits.

2. ACCESS CONTROL – All computers or devices connecting to District technology resources shall have access control that restricts the use to authorized persons.

3. CRITICAL AREAS – Critical technology equipment including, but not limited to, telephone cabinets, switches, servers and wiring racks shall be kept in locked areas. This equipment shall include uninterrupted power supplies, surge protection, and environmental controls for temperature and humidity where applicable.

4. STANDARD CONFIGURATION – Hardware and software will be configured by vendors and/or technology support personnel in a known and documented manner that can be easily restored if necessary.

5. NETWORK RESOURCES – Use of the school network shall be in a manner as to conserve the resources of the network. This includes traffic generated on the network, as well as files saved on servers. Individuals are expected to remove old and unnecessary files from network storage. Student files will be deleted 30 days after the end of each school year.

6. PRINTING LOCATIONS – Printers shall be strategically located for ease of use and to reduce maintenance and hardware costs. Document

printing centers shall be the primary location to print documents in excess of 10 pages. These locations will be determined by building administrators. Printing more than 10 pages at a time using a printer other than the printing center may be subject to review by building and department administrators.

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

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

9. RESPONSIBILITY FOR INTERNET USE – Each individual has the responsibility to avoid inappropriate sites, and to report any occurrence of inappropriate internet use to building staff or administration. Although systems to block access to inappropriate internet sites are in place, it is not possible to block all sites that may contain inappropriate or undesirable material. 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 an 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.

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

11. LIMIT PER PERSON – Staff is limited to a maximum of one computer per user for most user groups and shared computers for others. The director of technology is responsible for designating standard issue technology by employee classification group and for keeping technology up to date.

E. STAFF, STUDENT AND TENANT NETWORK ACCESS AND ACCOUNTS

TECHNOLOGY SUPPORT PROVIDER – The District technology support team shall support network accounts, network resources, passwords and

software/hardware maintenance. Building staff shall report all technology support requests to the technology support provider via the District help desk system. District technology support staff shall initiate or coordinate basic repairs on equipment and/or coordinate requests for repair or network services in a timely manner.

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

   - Each user shall be authorized to use the adequate features necessary rather than all available features possible.

   - Accounts shall be accessible via an intranet portal for access in and away from school.

   - Students no longer enrolled in Richfield Public Schools will have limited account access upon leaving the District, and their accounts permanently removed 30 days after being unenrolled or on June 30 of the school year they are last enrolled, whichever occurs first.

   - Staff no longer employed in Richfield Public Schools will have limited account access upon ending employment with the District either voluntarily or involuntarily, and their accounts permanently removed 30 days after ending employment or on June 30th of the school year they are last employed, whichever occurs first.

2. TENANTS' ACCOUNTS – Tenants and other non-authorized users of District facilities desiring access to the network must follow District operating procedures in obtaining and maintaining network access and accounts.

3. LOG OFF – Employees should log out of accounts when finished with their use. Computers should be turned off or locked whenever an employee walks away from their work station. Logged on computers should never be left unattended at workstations.

4. PASSWORDS – Staff and students are expected to use passwords and keep them secure. Automated systems shall periodically expire passwords, yet notify users that passwords are about to expire. Individuals are expected to respect the privacy and security of others. Persons should not watch when others are entering their password. Users should not write passwords where others may access them and should change a password as soon as possible if they suspect someone else knows it. New password creation and management structures such as multi factor authentication (MFA) may be enforced at any time by the District technology department with a 30 day prior notice to affected users.

5. PERSONAL BACKUPS – Storage will be available on District computers or servers to support the instructional activities of staff and students. All

individuals are encouraged to make backups of their important work, since files on District computers cannot be guaranteed.

6. UNAUTHORIZED USE OR ACCESS REVOKING ACCOUNTS – Depending on the nature and degree of the violation and the number of previous violations, unacceptable use of the District's 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 applicable District policies, including suspension, expulsion, exclusion or termination of employment; or civil or criminal liability under other applicable laws.

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

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

- Staff: temporary suspension of an account by an administrator or designee in accordance with provisions of employee contracts.

- Students: network and email privileges may be temporarily suspended by a supervising staff member, or suspended for a period of time not to exceed one (1) school year by building administration according to the school's discipline policies.

7. INTERNET USE AGREEMENT AND DISCLAIMER
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 District.

- An internet use agreement form for students must be read and physically or digitally signed by the user and the parent or guardian annually. The internet use agreement form for employees must be digitally signed annually by all employees.

- All users shall be notified of the District policies relating to internet use. Notification shall include:
  - Disclaimers limiting the District's liability
  - A description of privacy rights and limitations
  - Notification that means used to limit student access do not provide a fool proof means for enforcing provisions of this policy
  - Notification that violation of the acceptable use policy may result in revocation of privileges, school disciplinary action or other appropriate legal action

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

F. SOFTWARE

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.

- The ability of technical support staff to administer and maintain the equipment.

- The ability to operate and communicate with the existing network configuration in place or being developed at the time of acquisition.

- The ability of the District to maintain low total cost of ownership (TCO), to include initial purchase cost, device security, ongoing maintenance costs, costs for necessary and/or desired software, and purchase of replacement parts.

3. APPROVAL PROCEDURES – All purchases of instructional and non-instructional software, computer, and video and media hardware must be approved by the director of technology before being placed in the District's order entry system. The director of technology will also approve re-installation of previously removed software after verification that such software aligns with current curriculum and student objectives, as well as wider District strategic goals.

   All purchases of network infrastructure hardware and software must be approved by the District's technology support department before being placed in the District's order entry system.

   All potential donations of computer technology or equipment must be approved by the director of technology and director of finance before being accepted and added to the District equipment inventory system. Technology support personnel shall assist in the evaluation of donated equipment prior to its acceptance by the District.

4. TECHNOLOGY SPECIFICATIONS – Technology specifications shall be developed and updated at appropriate intervals to reflect current software and workstation requirements for new and donated equipment.

H. HOME USE OF COMPUTERS

1. AUTHORIZED USERS – Current employees and students of the District may, upon completion of proper forms or procedures as developed, use school computer, technology and/or electronics equipment at their home for school use.

2. CHECKOUT PROCEDURES –School technology equipment should not be signed out to any staff or student for home use unless designated as a personal issue device. This is limited to a laptop for staff and a

Chromebook and/or wireless hotspot for students. No other technology should be issued for home use.

I. USE OF PERSONAL DIGITAL DEVICES AT SCHOOL WORKSITES

1. AUTHORIZED USERS – Current employees, students, and authorized visitors of the Richfield Public Schools may, with prior approval, use their personal digital devices for school related tasks on the District's guest network.

2. INSTALLATION, MAINTENANCE AND REMOVAL

   - The date when equipment is added to the District network will be recorded.

   - Personal computers or digital devices shall not be repaired, maintained, nor have other hardware changes or additions provided by District staff.

   - The District is not liable for any damages or loss (including theft) to personal property that may result from the use of personal equipment at the school work site.

J. STAFF USE OF EMAIL, CHAT, VOICEMAIL, PHONE AND FAX

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

2. VOICE MESSAGES– Voicemail messages are not backed up or archived by network personnel. Messages are automatically deleted after 90 days.

3. STAFF EMAIL AND CHAT - Staff email and chat is archived for a period of three (3) years from the date the message was sent or received.

4. STUDENT EMAIL AND CHAT - Student email and chat, sent or received, is archived for a period of one (1) year from the date the message was sent or received, or upon removal of the account, whichever comes first.

5. MESSAGES ARE NOT PRIVATE – Messages stored on District systems or District authorized systems shall not be considered private property and may be accessed by District administrative employees. This would generally be done to resolve technical problems or at the request of administration.

6. CONSERVE RESOURCES – Individuals should use the voicemail, email and fax systems in a manner to conserve resources

7. AVOID AUTOMATIC FORWARDING – Emails sent to District email addresses should not be setup to automatically forward to external email locations in order to avoid the distribution of sensitive student or employee information.

8. 900 NUMBERS – Calls to 900 numbers shall not be permitted.

K. WEBSITE MANAGEMENT

1. WEBSITES – Schools and District programs shall have the opportunity to post content on the official school and District websites to enhance communication with students, families, and the community. These websites were established within systems agreed upon by the director of marketing and communications, the director of technology, and the District Technology Advisory Committee (DTAC).

   a. Intranet: An internal "intranet" website will be maintained for uses specific to internal Richfield Public Schools authorized users. Technical management of the intranet will be done by the communications department and the technology department. Content for the site will be determined by District administration. Teachers, building staff, and building administration may provide recommendations for additional site content.

2. WEBSITE PUBLISHING RIGHTS – The director of marketing and communications and the director of technology have the responsibility for granting publishing rights to District or school websites. These rights may be extended to employees, students, parents/guardians and/or community members. Training shall be provided to all users prior to granting of publishing rights to ensure effective use of the system, and to emphasize proper etiquette and accepted format to professionally and appropriately represent Richfield Public Schools. Training includes, but is not limited to, ADA compliance in web content, AP Style, and District brand guidelines. Employees should not create public, school-related websites outside of the official school or District websites. Teachers should use school-approved learning management systems for communicating with students and families. If educators or other District staff create Google sites for communication purposes, they should be set to be visible only to District students and staff; they should not be public.

3. WEBSITE CONTENT EXPECTATIONS – Teaching staff, program leaders, and administrators are expected to provide up-to-date website content with information of interest to District staff, students and the community. Expectations shall be developed by the director of marketing and communications and District administration, monitored at the building level by building administration.

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

Dated: February 5, 2001

Reviewed: November 4, 2007; April 6, 2015; August 16, 2021; September 6, 2022; September 16, 2024; August 18, 2025

Revised: November 20, 2006; April 19, 2021; September 5, 2023