

INTERNET RESOURCES

As a public school district committed to providing its employees and students with the necessary resources and skills to engage in a technically-literate society, it is important that Rio Rancho Public Schools lead by example. In order to provide better communication with district employees, students, parents, administration and the community, the district has integrated the use of the internet and intranets in the educational environment. As these technologies advance and improve the access to professional and personal communications so do the risks of abuse of district technologies and resources and other types of actions that violate district policies and federal and state laws and regulations. The board has developed this policy to ensure that district technologies and internet and intranet resources are used for professional and educational purposes that support and advance the mission of the district and provide a safe educational environment for students.

The provisions contained in this policy are intended to supplement, not supersede, existing district policies. Users of the district's internet and intranet resources are responsible for complying with all applicable federal, state and local laws and regulations, including, but not limited to the Children's Online Privacy Protection Act (COPPA); Family Educational Rights and Privacy Act (FERPA), and intellectual property laws. All district policies that govern employee conduct may be applicable to the types of conduct and interactions addressed in this policy.

A. Websites

1. District Website

The district website (www.rrps.net) and its individual web pages (collectively referred to herein as the "district website") will adhere to the following guidelines in addition to all other applicable district policies:

- a. The district website is the property of RRPS.
- b. All information on the district website shall be supervised and controlled by RRPS.
- c. The Superintendent or his/her designee shall have authority to approve or disapprove all information on the district website.
- d. The district website shall not be used as an open forum for public speech. Rather, the district website is intended to provide information to students, parents, staff, and community members in a manner similar to that distributed by the district in written paper format.

- e. The district website may include:
 - i. Accountability data and District Report Card;
 - ii. General information about the district and its schools;
 - iii. School schedule(s);
 - iv. District/school policies;
 - v. Calendar(s) of district/school events;
 - vi. Names, school phone numbers, and/or school e-mail addresses of school administrators and staff;
 - vii. Information otherwise available in student and parent handbooks;
 - viii. Other information deemed to be of interest to students, parents, and district employees by the Superintendent or his/her designee.
- f. To protect the safety and privacy of district students, the district website shall not include:
 - i. Student names, addresses, phone numbers, or e-mail addresses without permission from the student's parent or legal guardian;
 - ii. Photographs/videos where individual students are recognizable without permission from the student's parent or legal guardian;
 - iii. Student information and student records protected by FERPA or other federal and state laws relating to student privacy rights; and
 - iv. Other information deemed by the Superintendent or his/her designee to be inappropriate for publication.
- g. In order to protect the safety and privacy of district employees, the district website shall not include:
 - i. Staff home phone numbers and home addresses;
 - ii. Any other information deemed by the Superintendent or his/her designee to be inappropriate for publication.
- h. Only authorized district personnel may add or make changes to the district website.

2. Other District-related Educational Websites

The Board recognizes that district staff or students may create websites or web pages for school-related, professional purposes, such as for individual classes, class projects, or school-sponsored activities (collectively, “educational websites”). Educational websites shall adhere to the same guidelines for the district website, listed above. In addition:

- a. Student-created educational websites must be approved by the student’s teacher or adult sponsor and the school principal or designee.
- b. Student-created educational websites may include only a student’s first name.
- c. Student-created educational websites may not include a student’s address, telephone number, e-mail address; family or friends’ names or contact information; photographs/videos of the student without approval of the student’s parent or legal guardian; photographs/videos of any other staff member without the approval of the person depicted; nor photographs/videos of a member of student’s family or other district students, without the approval of the person depicted, if said person is at least 18 years old, or of the person’s parent or legal guardian. The teacher or adult supervisor who supervises the student’s education website shall collect and maintain the written authorizations.
- d. Staff-created educational websites may include the staff member’s name, school, school telephone number(s), and school e-mail address.
- e. Staff who create educational websites shall ensure that all students have access to the materials and information communicated on the educational website.

3. Unauthorized Changes Prohibited

Any person who knowingly, willfully or without authorization directly, or indirectly alters, changes, damages, disrupts or destroys any web page(s) or information, graphics, or pictures/videos on the district website, educational websites, or other websites or web pages on the district’s server may be referred to the law enforcement agencies. Additionally, students involved in such activity shall be subject to the district’s student discipline procedures, up to and including suspension or expulsion. Employees involved in such activity shall be subject to employee discipline, up to and including discharge or termination.

B. Educational Use of Social Networking Websites

Social media technology can serve as a powerful tool to enhance education, communication, and learning. The board is committed to ensuring that all district students

and staff who utilize social media technology for educational purposes do so in a professional, ethical, safe and responsible manner. The Board strives to create educational social media environments that complement the safe, educational environment of the classroom. This policy applies to professional, educational communications by district employees, as well as social media communications between district employees and students. This policy does not address personal, student-to-student communications using social media.

1. Definitions

- a. Social media includes, but is not limited to, any form of online publication or presence that allows interactive communication, including, but not limited to, social networks, blogs, microblogs, Internet websites, networking sites, photo/video sharing sites, Internet forums, and wikis.
- b. Educational social media: Educational social media includes both work- and school-related social media activity that is either school-based (e.g., a district teacher establishing a blog for his/her class), or administration-based (e.g., a Facebook page established by the district's central office to facilitate communication of district-wide announcements).
- c. "Communication" or "communicates," as used in this policy, refers to communication activities through social media technology, including, but not limited to, "friending," "following," "tweeting," "commenting," and "posting messages" using social media sites.
- d. Blogs refer to sites that can function as ongoing journals with multiple entries. Typically, entries are categorized with tags for easy searching. Most blogs allow for reader comments. Examples: Blogger, Wordpress, TypePad.
- e. Micro-Blogs refer to blogs that allow for shorter content posts, typically with a limited set of typed characters allowed. Micro-blogs can be used for status updates and to quickly communicate information to friends or followers. Examples: Twitter, Tumblr.
- f. Networking sites refer to those sites that allow people to connect with each other around common interests, pursuits and other categories. Examples: Facebook, LinkedIn, Google+, Ning.
- g. Photo/video sharing sites refer to those sites that allow people to share videos, images, slideshows and other media. Often these sites allow viewers to comment and share posted content. Examples: YouTube, Vimeo, Flickr.

2. Educational Social Media Use

- a. Maintenance of separate professional and personal e-mail accounts: District employees who receive approval from the Superintendent or designee to engage in educational social media activities shall maintain separate professional and personal email addresses. District employees shall not use their personal email address for educational social media activities. The educational social media site shall utilize an email address issued by the district's IT Department and shall be completely separate from any personal social media presence maintained by the district employee.
- b. Communication with district Students: District employees who communicate with students through educational social media sites shall comply with these guidelines:
 - i. On educational social media sites that communicate with district students, employees shall only use the sites for educational purposes that support the school's mission, curriculum and authorized activities. District employees are not to review any personal social media accounts created by their students.
 - ii. Educational social media sites that are school-based should be reasonably related to instructional, educational or school-sponsored extra-curricular program matters.
 - iii. Educational social media sites that are administration-based should have a reasonable relationship to the mission and function of the district.
- c. Employees shall obtain the prior approval of the Superintendent or his/her designee before setting up an educational social media presence.
- d. Principals and their designees are responsible for maintaining a list of all educational social media accounts within their particular school or office.
- e. The school principal shall be given administrator rights or access to educational social media accounts established by district employees at the school site.
- f. Each school year, district parents or legal guardians will be notified about the educational social media activities their children will be invited to participate in. Each school site shall inform parents of the purpose and nature of each educational social media account their children will have access to and will instruct parents to contact the school's principal or designee with any questions or concerns.

- g. Educational social media sites shall include language identifying the sites as educational social media sites of the district. For example, the educational social media sites can identify the district school, department or particular grade that is utilizing the site.
- h. District employees shall treat educational social media sites and communications like a classroom and/or a professional workplace and classroom setting. The same ethical and professional standards expected in district professional settings are expected on educational social media sites. If a particular type of behavior is inappropriate in the classroom or a professional workplace, then that behavior also is inappropriate on the educational social media site.
- i. District employees should exercise caution, sound judgment, and common sense when using educational social media sites.
- j. District employees should use privacy settings to control access to their educational social media sites to ensure that educational social media communications only reach the employee's intended audience. However, employees should be aware that there are limitations to privacy settings. Private communications published on the internet can easily become public. Furthermore, social media sites can change their current default privacy settings and other functions. As a result, employees have an individualized responsibility to monitor the educational social media sites they maintain and to understand and comply with the rules and terms of service of the social media site being utilized.
- k. Educational social media communications should be in compliance with district policies and applicable laws, including, but not limited to, prohibitions on the disclosure of confidential and personally identifiable information under FERPA and prohibitions on electronic communications that may be reasonably perceived as bullying, harassing, obscene, discriminatory, defamatory or threatening.
- l. District students who participate in educational social media sites may not be permitted to post photographs/videos featuring themselves or other students, without permission of the parent or legal guardian of the student depicted.

3. Monitoring of Educational Social Media Sites

- a. Employees using educational social media have no expectation of privacy with regard to their use of such media. The district will regularly monitor educational social media sites to protect the school community.
- b. District principals, or their designees, are responsible for monitoring use of educational social media sites by employees at their school site. The monitoring responsibilities include, but are not limited to, reviewing the educational social media sites on a regular basis. If supervisors discover questionable

communications or behavior on educational social media sites, the supervisors are required to contact the Superintendent or his/her designee.

- c. The district has the right to remove, disable, and provide feedback regarding educational social media sites that do not adhere to federal or state laws or regulations or district policies.
- d. Educational social media sites shall be created and maintained as a private network. The Superintendent or designee shall have the authority to determine whether an educational social media site should be maintained in a non-private manner to allow the larger district community to access the site.

4. Personal Uses of Websites, Social Media, and other Electronic Communications

In recognition of the public and pervasive nature of the internet and social media communications, as well as the fact that in this digital era, the lines between professional and personal endeavors are sometimes blurred, the following guidelines also address the board's expectations and recommended practices for use of personal websites, social media, and other electronic communications by district employees. "Personal uses of electronic communications" refer to an employee's use of non-district email accounts, text messages, instant messages, or any other form of communication that requires an electronic device to transmit.

a. Prohibited Conduct

District employees shall be aware that personal uses of websites, social media sites and electronic communications, even when such conduct falls outside of the regular duty day and is not transmitted on or through district-owned and controlled resources, have the potential to result in disruption at school and/or the workplace, and result in violations of district policies and federal and state laws and regulations. Examples of conduct that may result in disciplinary consequences up to and including termination or discharge include, but are not limited to, the following:

- i. Unauthorized personal uses of websites, social media, or electronic communications on district-owned computers, devices or networks.
- ii. The unauthorized posting, communication or disclosure of personally identifiable information of district students or other information maintained by the district as confidential information.
- iii. The unauthorized use or posting of any district logo, link to district websites or posting of district material.

- iv. Engaging in communications with currently enrolled district students using personal websites, social media or electronic communications, unless the district employee and student are relatives or the district employee reasonable believes in good faith that such communication is necessary to promptly respond to or communicate an emergency.

If district employees receive a request from a currently enrolled district student to connect or communicate through the employee's personal website, social media, or other electronic communication, district employees should refuse the request. The following language is one suggested response: "Please do not be offended if I do not accept or respond to your request. As a district employee, district prohibits personal interactions with currently enrolled district students on personal websites, social media, or through personal electronic communications. If you do want to connect, please contact me using my school contact information at _____."

As of the effective date of this policy, employees who use personal websites and social media sites shall remove currently enrolled students, other than their relatives, from their "friend," "follower," or other type of contact lists on their personal websites or social media sites.

- v. Use of personal websites, social media, or electronic communications for conduct that otherwise violates district policies (e.g., harassment, bullying).

Rio Rancho Public Schools
Adopted: June 11, 2018
Effective Date: July 1, 2018

Previous policies adoption history:

Adopted: August 9, 2010
Adopted: September 20, 1999
Revised: June 11, 2012