

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 the goal of the Board that Pojoaque Valley 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 the risks of abuse of District technologies and resources also increase, as does the risk of other types of misconduct 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 by staff and students for professional and educational purposes that support and advance the mission of the District and promote 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. The District Website.

The District website (www.pvs.k12.nm.us) and its individual webpages (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 the District.
- b. All information on the District Website shall be supervised and controlled by the District.
- c. The Superintendent or his/her designee shall have authority to approve or disapprove all information on the District Website.
- d. 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, positions, 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 relating to the District which are 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, personal or home phone numbers, or e-mail addresses without express, written permission from the student's parent or legal guardian;
 - ii. Photographs/videos where individual students are recognizable without express, written permission from the student's parent or legal guardian unless such images are considered Directory Information;
 - iii. Other 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. The District recognizes the importance of community access to its children's educators. However, 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 or personal email addresses;
 - ii. Photographs/videos where individual staff members are recognizable without their express, written permission; and
 - iii. 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 of Education recognizes that District staff or students may create websites or webpages 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 **shall not** include a student's address, telephone number, e-mail address; family or friends' names or contact information; photographs/videos of the student without express approval of the student's parent or legal guardian; photographs/videos of any other staff member

without the express approval of the person depicted; nor photographs/videos of a member of student's family or other District students, without the express 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 webpages 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; Staff Responsibilities.

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 compliment 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 include personal, student-to-student communications using social media outside of the school premises that may negatively impact the learning environment. Initial use of any social media must be approved by the appropriate site Principal or designee.

1. Definitions.

- a. **Social Media.** 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** means school-related social media activity that is either classroom-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 Accounts.** District employees who receive approval from their site Administrator 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 as a communication medium for any school related business. 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 may communicate with students through Educational social media sites that are school-based for purposes that are reasonably related instructional, educational or school-sponsored extra-curricular program matters. In such communications, employees shall comply with these rules:
 - i. Employees shall only use the sites for educational purposes that support the school’s mission, curriculum and authorized activities.
 - ii. Educational social media sites that are administration-based should have a reasonable relationship to the mission and function of the District office creating the social media account.

- iii. Employees shall obtain the prior approval of the site Administrator or his/her designee before setting up an Educational social media account.
- iv. Principals and their designees are responsible for maintaining a list of all Educational social media accounts within their particular school or office.
- v. The school principal shall be given view access to the Educational social media accounts established by District employees at the school site.
- vi. District parents or legal guardians will be notified about the Educational social media activities their children will be invited to participate in. Each classroom teacher 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 classroom teacher with any questions or concerns.
- vii. 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.
- viii. All 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 which apply to other employee activities also apply 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.
- ix. Employees have an individualized responsibility to monitor the Educational social media sites they maintain and shall immediately report to the District's IT administrator and the employee's supervisor any activity that indicates privacy settings have been affected or unauthorized access to the site has occurred
- x. Educational social media communications shall comply 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.
- xi. District students who participate in Educational social media sites may not be permitted to post photographs/videos featuring themselves or other students who could be readily identified, without the express permission of the parent or legal guardian of the student depicted. This would be

permission above and beyond the parent permission obtained at the beginning of the school year.

c. Monitoring of Educational Social Media Sites.

- i. 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.
- ii. 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 a supervisor discovers questionable communications or behavior on Educational social media sites, the supervisor shall immediately contact the Superintendent or his/her designee.
- iii. 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, District policies or contain material that is otherwise inappropriate in or disruptive to the District's educational program.
- iv. To assist in monitoring, the default setting for comments on Educational social media sites shall be turned "off."
- v. Educational social media sites shall not be created and maintained as a public network.

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

"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 between a student and a District employee 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.
- v. Use of personal websites, social media, or electronic communications for conduct that otherwise violates District policies (e.g., harassment, bullying).