STUDENT USE OF DISTRICT TECHNOLOGY 371

Purpose

The Pojoaque Valley School District provides access to electronic networks, including access to the Internet, as a part of the District's instructional program to enhance teaching and learning. The use of the District's property must be for educational and research purposes consistent with the educational objectives of the District. The District reserves the right to monitor and access all use of or content on the District's computers and networks. No person or user has an expectation of personal privacy in connection with their use of or content stored in, created, received or transmitted over any District property, including its computers and networks, unless such right is guaranteed by statute or other law. The Superintendent is delegated the authority to promulgate guidelines and user agreements consistent with this policy and as necessary to reflect technology development.

A. Prohibited Use.

In order to protect the integrity of the District's property and to protect the interests of the District and its students, the District prohibits (1) use that causes congestion or disruption to the District's computers and network; (2) searching, retrieving, transmitting or viewing any content in emails or other communications or documents that are not intended for that person (3) unauthorized software use or downloading or installing unauthorized software, programs or files; (4) use of the network for non-District business including commercial activities, product advertisement, financial gain or political activity; (5) engaging in any illegal or inappropriate conduct, including but not limited to copyright infringement, plagiarism, piracy, harassment, intimidation, threats, defamatory conduct, or misrepresentation including the unauthorized use of passwords or identities of other persons.

B. Student Responsibilities.

Students are responsible for exercising good behavior when using District computers and networks, and users are responsible for complying with all District policies when using District computers and networks. Students are expected to take responsibility for conducting themselves in an appropriate, efficient, ethical, and legal manner when using the District's hardware, software, network resources, and accessing the Internet. Students shall be responsible for handling the District's equipment in a prudent manner in order to protect it from damage.

The use of information technology resources is a privilege, not a right. Any student's failure to exercise good behavior, to comply fully with this policy or to fail to fully comply with other District policies will warrant serious consequences including, but not limited to, loss of computer and network privileges, discipline, suspension, expulsion, and legal action or money damages for repair or replacement of equipment. Users are notified that sexually explicit or pornographic content has no place in the District and violators who use or access such content will face severe consequences including expulsion and legal action.

C. District Security Measures

The Internet provides access to a wide range of material. The District expects that staff will blend thoughtful use of the Internet throughout the curriculum. Because technology is constantly evolving, it is impossible for school personnel to review and pre-select all materials that are appropriate for the use of students and employees. The District approaches appropriate Internet usage in the following ways:

1. **Filtering** – To the extent possible, the District shall use commercially reasonable technology protection measures that allow it to meet the requirements of the Children's Internet Protection Act, including the use of a filter to protect against access to:
a. Material that is, by definition, obscene (section 1460 of title 18, U.S. Code)
b. Child pornography (section 2256 of title 18, U.S. Code)
c. Material that is harmful to minors (further defined in the Children's Internet Protection Act)

2. **Supervision** – Since no technology protection measure will block 100 percent of the inappropriate material, the District emphasizes the importance of supervision. It is the expectation that all Pojoaque Valley School District staff will be responsible for monitoring and supervising all users of information technology resources, including the Internet.

3. **Education** – Education about online behavior, including interacting on social networking sites and chat rooms, as well as issues surrounding cyber-bullying awareness and response, will be covered in the curriculum each school year.

D. Administration, Monitoring, and Privacy Rights

The District owns its computers, its networks and the content on those computers and networks. The District may enforce the operation of technology protection measures at any time and during any person's use of the District's network. To insure system integrity and appropriate use of information technology resources, the District reserves the right to monitor, inspect, store, and copy any information transmitted, stored, or received using information technology resources. Users shall have no expectation of privacy regarding the use of or content in information technology resources. In certain limited circumstances reserved to the discretion and decision of the Superintendent or the Superintendent's designee (an administrator or other authorized person), the technology protection measures may be disabled, circumvented, or minimized for those demonstrating a bona fide research need to access such filtered or blocked materials, or for other lawful purposes.

E. Statement Prohibiting Use Related to Discrimination, Harassment, and Defamation

The District prohibits use of its computer system for any purpose in violation of the District's discrimination and anti-harassment policies. All forms of harassment through the use of technology commonly referred to as cyber-bullying, are unacceptable and viewed as a violation of this policy. Cyber-bullying includes, but is not limited to the following misuses of technology: harassing, teasing, intimidating, threatening, or terrorizing another person by sending or posting inappropriate and hurtful email messages, instant messages, text messages, digital pictures or images, or website postings. The District's computer system may not be used to defame others or disclose sensitive personal information about others.

F. Copyright Infringement of Software

The District prohibits the unauthorized use, downloading, installation, or copying of software on the District's computer system. All software used, downloaded, installed or copied must be approved by the District. All users must comply with applicable licensing agreements and copyright laws, and copyrighted material may not be used or shared without authorization from the publisher.

G. Electronic Communication Devices during Testing

During the PVSDs' student participation in State mandated assessments such as the annual New Mexico Standards-Based Assessments (NMSBA) and other short cycle assessments, students are not allowed to:

- have electronic devices, inclusive but not limited to, cell phones, in their possession during any testing sessions
- have any electronic devices, inclusive but not limited to, cell phones, outside of their backpacks during testing
- have any electronic devices powered "on" during any testing periods
- place backpacks anywhere in the classroom other than in the front of the room

Test Administrators and Proctors MUST have cell phones or any other electronic devices off or on vibrate during testing sessions. Test Administrators and Proctors are responsible for monitoring, relocating and reporting all breeches of procedure.

H. Description of Other Unacceptable Uses

District resources are to be used for school-related administrative and educational purposes. The user is responsible for his or her actions and activities involving technology. Some examples of prohibited uses include, but are not limited to, the following:

1. Searching for or deliberately viewing, listening to or visiting websites with or known for containing inappropriate material or any material that is not in support of educational objectives, such as profane material, obscene material, sexually explicit material, or pornography.
2. Attempting to vandalize, damage, disconnect or disassemble any network or computer component.
3. Attempting to gain unauthorized access to the District system or to any other computer system through the District system, or beyond an individual's authorized access. This includes attempting to log in through another person's account or accessing another person's files with or without the person's permission.
4. Searching for or creating security problems will be construed as an unauthorized attempt to gain access, i.e., computer hacking.
5. Using District resources for purposes of plagiarism, theft, infringement and other illegal or illicit purposes.
6. Connecting personal property to District equipment or network, including using personal cellular/mobile technology (i.e., iPhone, Blackberry) devices to access the District's property, networks or Internet access without prior written authorization.
7. Installing software without permission of the Director of Technology or his/her designee or using District software in a manner inconsistent with the District's interests, license agreements and applicable laws.
8. Wasting District resources including bandwidth.
9. Bypassing or attempting to circumvent network security, virus protection, network filtering, or policies.
10. Using District resources to access personal or third party files, information, or electronic mail such as hotmail, yahoomail, gmail, etc.
11. Revealing personal data of students and staff (example: PIN, social security number, credit card numbers, addresses, phone numbers, etc.),
12. Using the system for purposes unrelated to the interests of the District such as use for commercial purposes or personal pleasure or gain.

In the event a user has any questions regarding whether a use of the District's property is appropriate under this Policy, then the user must contact the Technology Coordinator for direction.

I. Use of Social Networking Sites

Certain Web 2.0 services, such as Moodle, wikis, podcasts, RSS feeds and blogs that emphasize online educational collaboration and sharing among users, may be permitted by the District. However, such use must first be approved by the Technology Coordinator or designee, followed by training authorized by the District. Users must comply with this policy as well as any other relevant policies and rules during such use.

J. Monitoring, Supervision, Enforcement, and Penalties

Consequences of violations of the AUP include, but are not limited to, the following:
• Suspension of network privileges
• Revocation of network privileges
• Suspension of Internet privileges
• Revocation of Internet privileges
• School suspension
• School expulsion
• Restitution for the cost of the repair and/or technician fees to repair or replacement costs
• Legal action and prosecution by the authorities.

K. Disclaimer of District Responsibility

The District makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District will not be responsible for any damages the student suffers, including but not limited to, loss of data or interruptions of service. The District is not responsible for the quality of any information obtained through the Internet or stored on the network. Internet sources used in student papers, reports, and presentations should be cited in the same manner as references to printed materials. The District will not be responsible for financial obligations arising through unauthorized use of the network. Students shall agree to defend and hold the District harmless from any losses sustained as a result of intentional misuse of the network.