JAL PUBLIC SCHOOLS
TECHNOLOGY DEPARTMENT
www.jalnm.org 200 E. Panther Ave. • PO Box 1386 • Jal, NM 88252 • Office: (575) 395-2379 • Fax: (575) 395-2146

Computing and Internet Acceptable Use Policy

Teachers and students attending Jal Public Schools have the privilege to use technological tools to help them excel in their jobs or course work, while also providing the opportunity to communicate electronically with other schools, organizations, and individuals around the world. With this opportunity also comes responsibility. The Internet is a vast array of information networks. While most of this information is useful and appropriate, there are times when a user may encounter material or information that can be offensive, illegal, or obscene, etc. While the District takes every precaution to curb such access and does not encourage this contact, it is not 100% possible to prevent it. That is also why the District incorporates Internet Safety into its curriculum, and encourages users to report inappropriate content to teachers or other school officials. Deliberate misuse of the District's technology resources can result in the temporary or permanent loss of privileges to technology tools within the District's private network.

A. Purpose

a. Jal Public Schools provides its employees and students ("Users") with access to computing equipment and local network functions such as District email and the Internet.
b. This access has a limited education purpose for students and is to facilitate work productivity for employees.

B. Access Rights and Privileges

a. The School District has the right to place reasonable restriction on the use of equipment, resources, and materials students and employees access or post through the system. Students and employees are also expected to follow the rules set forth in the District's rules and regulations governing conduct, disciplinary code, and the law in their use of the District's equipment and network. This access has not been established as a public access service or a public forum.
b. All access and rights are privileges granted by the District, and users should expect no privacy rights. District computers and other technological tools are to be used only for business or educational purposes. Users consent to allowing personnel of the District to access and review all materials they create, store, send, or receive on school equipment. Users understand that the School District may use human or automated means to monitor use of its computer resources.
c. All District employees and students will have access to the Internet through the District's private network. Parents may specifically request that their children not be provided such access by notifying the District in writing.
d. Guests/contractors are not automatically eligible for a District email account or network and Internet access. Such access may be granted if directly sponsored by a District Administrator.
e. Employees are expected to use their District-provided email accounts for school business purposes only. Any personal messages or information transmitted through the District-provided email is subject to review by District Administrators.
f. While students in grades 7-12 have privileges to District-provided email, such access will be closely monitored and limited to activity which only relates to classroom curricula or contact with higher education institutions. Any personal messages or information transmitted through the District-provided email is subject to review by District Administrators.
g. All Users should note that all computer labs that are not used for full-time instruction are monitored by 24-hour video surveillance.

C. System Security Obligations

a. Users are responsible for their passwords and for the use of their individual access account(s) and should take all reasonable precautions to prevent others from being able to use their account(s), including co-workers, friends, or family. Under no conditions should a user provide his/her password to another person, nor attempt to access the network with another User's password or account.
b. Attempts to log on to the District's network as a System Administrator are strictly prohibited.
c. Users must take reasonable precaution to ensure he/she does not introduce viruses to the School District's network. Any material received on flash drives, CDs, DVDs, or other media MUST be scanned for viruses or other destructive programs before being placed on a computer system within the District's network. Further, any detection of viruses, spyware, malware, or other destructive programs must be reported immediately to the Technology Department or to District Administrators.
d. Users should immediately notify a teacher or system administrator of any possible security breach.
e. Students will promptly disclose to their teacher or other appropriate school employee any message or file received that is offensive, illegal, obscene, profane, or in any other way inappropriate.
f. Users may not connect unauthorized wireless devices to the District network. Such devices include but are not limited to: wireless access points, wireless routers, or any other type of wireless gateway device.
g. Users may not install or use encryption software on any of the District's computers without first obtaining written permission from their supervisors. Users may not use passwords or encryption passwords that have not been provided to their supervisors.
h. Any user identified as a security risk or having a history of violating this or any other Acceptable Use Policy may be denied access to the District's network or other resources.

D. Filtering

a. As required by law, and in recognizing the need to establish a safe and appropriate computing environment, the District employs the use of filtering technology to prohibit access to objectionable or unsuitable content that might otherwise be accessible via the Internet.
b. In addition to filtering, the District also integrates Internet Safety courses into its curriculum.

E. Unacceptable Uses

a. Users may not use the District's private network to access material that is profane or obscene, that advocates illegal acts, or that advocates violence or discrimination towards other people.
b. Users may not use District equipment to post personal information on the Internet about themselves or other people. Personal contact information includes address, telephone numbers, school address, work address, pictures, videos, etc.
c. Users may not attempt to gain unauthorized access to any computer system. This includes attempting to log in through another person's account or access another person's files. These actions are illegal, even if only for the purpose of "browsing," "snooping," or "electronic discovery."
d. Users may not deliberately disrupt or harm hardware or systems, interfere with computer or network performance, interfere with another's ability to use equipment or systems, or destroy data.
e. Users may not use the District's private network to engage in illegal acts, such as threatening the safety of another person, accessing or sharing unauthorized copyrighted music, movies, and other intellectual properties.
f. Users may not utilize peer-to-peer file-sharing applications or execute programs to facilitate the downloading or exchange of copyrighted or unauthorized music, movies, or other materials.
g. Users may not use the District's private network to solicit information with the intent of using such information to cause personal harm or bodily injury to others.
h. Users may not post information that could endanger an individual, cause personal damage or a danger of service disruption.
i. Users may not knowingly or recklessly post false or defamatory information about a person or organization.
j. Users may not intentionally seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users.

k. Users may not indirectly or directly make connections that create “back doors” to the District’s network that allow unauthorized access from outside of the network.
l. Users may not use obscene, profane, lewd, vulgar, rude, inflammatory, hateful, threatening, or disrespectful language.
m. Users may not engage in personal attacks, including prejudicial or discriminatory attacks.
n. Users may not harass another person.
o. Users may not re-post a message that was sent to them privately without permission from the original author.
p. Users may not forward or post chain letters or engage in “Spamming” (sending large amounts of unnecessary mail to a large number of people). Users must also refrain from abusing email privileges by forwarding non-school/work related emails, advertising, and solicitations.
q. Users may not install or reproduce unauthorized or unlicensed software on District resources. Authorized software will be installed by authorized personnel only.
r. Users may not use technology resources and Internet for private business activities or unreasonable personal use.
s. Users may not use the District’s private network for political lobbying.
t. Students may not download any programs on District machines. File downloads are only allowed with teacher’s permission or if the file is necessary for an assignment.
u. Users may not use any type of internet proxy service or proxy server to bypass District web filters. Any such attempts will result in immediate revocation of computing and internet privileges.
v. Users may not alter machine configurations or attempt to perform unauthorized diagnostics or repairs on District machines. Diagnostics and repairs must be performed by or under the supervision of authorized personnel only.
w. Unless expressly authorized by District Administration, sending, transmitting, or otherwise disseminating proprietary data, trade secrets, or other confidential information of the School District is strictly prohibited. Unauthorized dissemination of this information may result in substantial civil liability as well as severe criminal penalties under the Economic Espionage Act of 1996.
x. Users may not alter the placement or positioning of computers, printers, and other technological equipment without consent of the Technology Department.

F. Due Process

a. The School District will cooperate fully with local, state, and federal officials in any investigation concerning or relating to any illegal activities conducted through the District’s private network.
b. In the event there is an allegation that a student has violated the District’s Acceptable Use Policy, disciplinary actions may be taken.
c. Employee violations of the District’s Acceptable Use Policy will be handled in accordance with law and School Board policies.

G. Administration

a. School Administration and Technology Directors have the responsibility and authority for the development, publication, implementation and ongoing administration and enforcement of the processes and techniques required to protect Jal Public School’s technology systems and services from unauthorized access, loss, or misuse.
b. School Principals have the responsibility to establish a plan to ensure adequate supervision of students. They are also responsible for interpreting and enforcing this policy at the local level.
c. Teachers and Staff have the responsibility to enforce and interpret this policy.