

RANCHO SANTA FE SCHOOL DISTRICT

Board Policy Number 5028: STUDENT USE OF DISTRICT'S ELECTRONIC RESOURCES

A. Purpose & Coverage

1. This policy defines the proper use by the students of the District of the District's electronic resources including, but not limited to, its computers, computer systems, and Internet access services.
2. This policy applies to all students of the District.
3. The Management Systems Information Manager for the District shall be the Superintendent

B. Overview of Policy Regarding Student Use

1. The District provides its students electronic resources such as computers for use as educational tools. The District recognizes that these resources present tempting opportunities for users to gain access to matters which are confidential, require restricted access, or which result in an improper use of the District's resources. It is the responsibility of each student to ensure that the District's electronic resources are used for legitimate educational purposes and in a manner that does not compromise confidential, proprietary or sensitive information. Students may not use or permit others to use the District's computer systems or other electronic resources for unlawful purposes. Such conduct should be reported and will not be tolerated. Misuse of the District's computer systems or other electronic resources will result in discipline, up to and including expulsion from school.
2. The District's computer systems and other electronic resources are District assets. There are numerous ways in which the improper use of these assets could jeopardize the proper operation of the District's computer systems and expose the District and its employees to liability in the event of a lawsuit. For example, use of the District's computer system for purposes unrelated to the District's educational curriculum compromises the remaining available memory of such systems and can slow the system's ability to process data effectively or in a timely manner. Viruses can damage the systems and stored information critical for the performance of District responsibilities. Use of the Internet and/or the electronic mail access provided to District employees to download or send obscene or discriminatory material could expose the District and its employees to liability for claims of sexual harassment or discrimination. For these reasons and others, students will not be provided access to electronic mail and student use of computers shall be under the direct supervision of a certificated employee at all times. In addition, technology protection measures have been installed which blocks or filters access to visual depictions that are obscene, child pornography or

other matter harmful to minors, and to chat rooms. These measures must be in force during any use of any District computer by minors.

3. In order to ensure that the District's computer systems are not misused, the District may randomly inspect and/or monitor computer files, District storage devices such as flash drives and discs, Internet use, and all other information stored or recorded by students on the computer systems to assure that these public resources are not being misused. Students should not expect that information kept on District computer system devices or equipment is private, even if the information is personal. Computer data may be monitored regardless of its origin or content. By utilizing the District's computer system devices and other electronic resources, a student consents to the monitoring summarized in this policy. Students are hereby placed on notice that the District is not responsible for any injury to students caused by others who may access such information.
4. The District reserves the right to take any action in order to comply fully with the provisions in 20 U.S.C.A. section 6777 (Internet Safety), including but not limited to, the use of technology protection measures to block student access to websites that contain obscene, pornographic or other material harmful to minors; and the use of technology measures to prevent hacking or any unlawful activities.

C. Definitions

1. The term "personal" or "personal information" as used in this policy refers to information unrelated to the student's academic pursuits, or other information which the student may not want disclosed to others.
2. The term "computer" includes any hardware, software, or other technology attached or connected to, installed in, or otherwise used in connection with a computer.
3. Access to the Internet shall include all District computers connected to a computer network and/or the Internet, and other personal electronic communication devices which access the District network and/or the Internet.
4. The term "child pornography" has the meaning given that term in federal and state case law and is prohibited if it is obscene or if it depicts actual children.
5. The term "harmful to minors" means any picture, image, graphic image file, or other visual depiction that taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex or excretion; that depicts, describes or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

6. The term "obscene" has the meaning applicable to that term under 18 U.S.C. section 1460.
7. The term "sexual act" and "sexual contact" have the meanings given those terms in section 2246 of Title 18.

D. Prohibited Student Access

Students will not be supplied with user ID's or passwords by employees of the District. Students shall be permitted to use only District computers which are equipped with technology protection devices designed to prevent access to child pornography, obscene materials or other materials harmful to children. Computers and the Internet shall be used by students only under the direct supervision of a certificated employee of the District.

E. Unacceptable Use

1. The use of the District's computer systems and other electronic resources is a privilege which may be revoked at any time. Computers, computer files, Internet services, software and other electronic resources are furnished to students for use in connection with the educational requirements of the District. All information stored or recorded on the District's computers shall be considered District property and may be retrieved and reviewed by the Information Systems Manager to insure the District's computer resources are not being misused. Students of the District cannot expect personal information recorded or stored on the District's computer resources to remain private. The District will not tolerate misuse of its electronic resources. Conduct which shall result in student discipline shall include, but is not limited to:
 - a. Causing malfunction, damage or theft of system hardware, software or components;
 - b. Altering system software or hardware;
 - c. Placing unlawful information, computer viruses or harmful programs on or through the computer systems;
 - d. Entering into restricted information or electronic mail on systems or network files in violation of this policy;
 - e. Violating the privacy of other computer system users;
 - f. Using another person's name and/or password and login to access the network or to send or receive messages on the network or Internet;
 - g. Violating the federal Communications Decency Act or any other federal or state law applicable to computer and/or telecommunications systems;

- h. Using the District's computer systems or other electronic resources for personal gain, profit, gambling, or commercial purposes, or to engage in any unlawful activity;
- i. Displaying or transmitting sexually explicit images, messages or cartoons which are obscene, child pornography or material harmful to minors;
- j. Using the District's computer system to unlawfully bully other persons;
- k. Displaying or transmitting messages containing ethnic slurs, racial comments, off-color jokes or anything that may conflict with the District's policy of providing an educational environment which is sensitive to diversity and free of harassment and disrespect;
- l. Unauthorized review, duplication, dissemination, removal, damage, or alteration of files, passwords, user IDs, computer systems, or programs, or other property of the District, a business, or any governmental agency to conduct activities commonly described as "hacking."
- m. Using copyrighted data or other materials without permission from the copyright holder, including, but not limited to use of data downloaded off of the Internet and the creation or maintenance of archival copies of materials obtained through the Internet, unless such materials are in the public domain.
- n. Obtaining, downloading, viewing or otherwise gaining access to materials which may be deemed unlawful, harmful, abusive, obscene, pornographic, descriptive of destructive devices, or which are harmful matter as defined in California Penal Code section 313(a), or which are otherwise objectionable under current District policies or applicable state or federal laws.
- o. Placing programs on computer systems without the permission of the District.
- p. Unless the prior approval of the Information Systems Manager has been obtained, using the Internet or other external network connections in a way that could allow unauthorized persons to gain access to the District's systems and information. These connections include the establishment of World Wide Web home pages and File Transfer Protocol.
- q. Placing District information of a confidential, sensitive or proprietary nature on the Internet.
- r. Illegally duplicating software or its related documentation.

- s. Accessing information other than that information which the student personally placed on an electronic resource, or which is publicly available, or which the student has been given authorization to access.
- t. Any activity prohibited by the No Child Left Behind Act of 2001 or state law.

F. Electronic Mail Rules

Access to the District's outsourced electronic mail service is a privilege designed to assist students in the acquisition of knowledge and in efficiently communicating with others. The electronic mail system is meant to be used for educational purposes. Electronic mail files are subject to monitoring by the Network Administrator. Use of the District's electronic resources to create or utilize chain letters, chat rooms or other Multiple User Dimensions ("MUDs") is forbidden, with the exception of those bulletin boards or electronic mail groups that may be used for specific educational-related communication. The District reserves the right to remove files from, or limit or deny access to, its electronic resources at any time.

All electronic mail correspondence is the property of the District.

Student electronic mail communications are not considered private despite use of passwords or any designation concerning privacy either by the sender or the recipient.

Electronic mail may not be used by students for personal gain, profit, commercial ventures, or gambling.

If not encrypted, electronic messages sent to recipients outside of the District's computer networks are not secure. Confidential, personal or proprietary information should not be sent in electronic messages.

The District has the right to monitor its electronic mail system, including each individual's mailbox, at its discretion in the ordinary course of business. In certain situations, the District may also be compelled to access and disclose messages sent over its electronic mail system to third parties. The District shall not be liable for any damages arising from any such disclosure.

The existence of passwords, user IDs and "message delete" functions do not restrict or eliminate the District's ability or right to access electronic communications.

Students shall not share an electronic mail passwords or user IDs, provide electronic mail access to an unauthorized user, or access another user's electronic mail box without authorization.

Students shall not post, display or make easily available any computer access information, including, but not limited to, passwords and user IDs.

Offensive, demeaning or disruptive messages are prohibited. This includes, but is not limited to, messages that are inconsistent with the District's policies concerning equal opportunity, sexual harassment, and other unlawful harassment.

Users must not use inappropriate language; language consisting of profanity, vulgarities or obscenities, language which libels others, or language which contains inappropriate references to others.

Users shall not reveal the residential addresses or telephone numbers of other individuals during electronic mail transmissions due to the lack of security of unencrypted messages.

Users may not use the District's electronic network in a manner which could damage, disrupt or prohibit the use of the network by other users.

Users should assume that all communications and information is public when transmitted via the network and/or Internet and may be viewed by others.

Users may not violate or permit the violation of the privacy or other rights of individuals whose information is required by or routinely stored by the District in computer systems or other electronic resources.

Users should exercise restraint in consuming shared electronic resources.

G. Internet Rules

1. The District's network, including its connection(s) to the Internet, is to be used for education-related purposes. Any unauthorized use of the Internet is strictly prohibited. Unauthorized use includes, but is not limited to: connecting, posting, or downloading pornographic material; engaging in computer "hacking" and other related activities; attempting to disable or compromise the security of information contained in District computers; or otherwise misusing the District's computers for illegal purposes or for any prohibited purpose as set forth in this policy as grounds for discipline.
2. Internet messages should be treated as non-confidential. Anything sent through the Internet passes through a number of different computer systems, all with different levels of security. The confidentiality of messages maybe compromised at any point along the way.
3. Because postings placed on the Internet may display the District's name and/or address, users must make certain before posting information on the Internet that the information reflects and is consistent with the standards and policies of the District. Before posting material online that is affiliated with the District or a District organization, including the creation of a social networking account or web page, prior written authorization of the Superintendent is required.

4. Subscriptions to news groups and mailing lists may be permitted when the subscription is for an education-related purpose. Any other subscriptions are prohibited.
5. Information posted or viewed on the Internet may constitute published material. Therefore, reproduction of information posted or otherwise available over the Internet may be done only by express permission from the author or copyright holder.
6. Unless the prior approval of Information Systems Manager has been obtained, users may not establish Internet or other external network connections that could allow unauthorized persons to gain access to the District's systems and information. These connections include the establishment of World Wide Web home pages and File Transfer Protocol.
7. All files downloaded from the Internet must be checked for possible computer viruses. If a user is uncertain whether their virus-checking software is current, they must check with the Information Systems Manager before downloading.
8. Downloading, sending or transferring offensive, demeaning or disruptive materials over the Internet is prohibited. This includes, but is not limited to, materials which are inconsistent with the District's policies concerning equal educational opportunity, sexual harassment, or any laws concerning harassment or discrimination.
9. Under no circumstances shall information of a confidential, sensitive or proprietary nature be placed on the Internet.

H. Reporting of Abnormalities or Misuse

1. All users are required to report any abnormality or security breach as soon they observe it or come into possession of information that it has occurred. Abnormalities or breaches of security shall be reported to the Information Systems Manager or Principal immediately. Users are also required to report any misuse of the District's computer systems. If any student observes a misuse, such as an electronic communication containing obscene or harassing language, the student should immediately report the misuse to the Information Systems Manager or Principal. Students should not show, transmit, or otherwise duplicate the misuse or offending material to, or discuss these matters with, anyone other than the Information Systems Manager or Principal.

I. Lack of Privacy & Monitoring

1. The Information Systems Manager shall have discretion to randomly monitor any information recorded or stored by students on the District's computer systems

upon approval by the Superintendent or designee. The Information Systems Manager may randomly retrieve and review all communications and electronically stored data on the District's electronic resources, whether that data be personal information, educational information, or information related to District business, in order to insure the District's property is not being misused. All information stored or recorded on the District's computers or other electronic resources shall be considered District property.

2. All students should be aware that information is available about their computer activities. Student computer activities are not private. For example, each time a student accesses a web site on the Internet, the computer and networking equipment involved create a trail, download and display the files from the Internet, and usually store a copy of those files on the hard drive. The computer or server that maintains the connection to the Internet also keeps track of which computer and which user has visited each specific web site. The District owns the computer terminals, services, networks and equipment and has the right to monitor student activities on the Internet at random.
3. If a student reports suspected misuse of the computer systems or other electronic resources to the Information Systems Manager or Principal. Upon receiving such a report, and/or if the Superintendent reasonably believes, in his/her sole discretion, that a student is misusing the District's computer systems or other electronic resource, the Superintendent may direct a designated District employee to review the suspected student's Internet use, or other electronically recorded use of the District's computer systems or electronic resources. In his/her discretion, the Superintendent may also report suspected misconduct to law enforcement officials and allow those officials access to the student's Internet use, or other electronically recorded use of the District's computer systems or electronic resources.
4. The District is not responsible for any injury to a student or any other person caused by third parties who may access personal information which the student has stored or recorded on the District's electronic resources.

J. Copyright Issues

1. The District purchases and licenses the use of various computer software for business purposes and does not own the copyright to this software or its related documentation. Unless authorized by the software developer, the District does not have the right to reproduce such software for use on more than one computer.
2. Students may only use software on the District's networks or on multiple machines in accordance with the applicable software agreement. The District prohibits the illegal duplication of software or its related documentation by students or by anyone else.

K. Vandalism

1. Vandalism is defined as any malicious attempt to alter, harm or destroy equipment, data or other property of the District or another user, or the networks connected to the District's networks via the Internet. This includes, but is not limited to, the uploading or creation of computer viruses, improper alteration of data, or the improper use of restricted information. Any vandalism of District computer systems or other electronic resources will result in disciplinary action, up to and including expulsion and, if appropriate, referral to law enforcement officials.

L. Consequences for Violating This Policy

1. The consequence for violating this policy include, but are not limited to, one or more of the following:
 - a. Disciplinary action up to and including expulsion;
 - b. Referral to legal authorities for prosecution under California Penal Code section 502 (unauthorized access to computers, computer systems and computer data), or other violations of state or federal laws.
 - c. Referral to legal authorities for prosecution under any applicable state or federal law.

M. District Not Liable for Damage to Student Work-Product

From time-to-time the District's computer systems will fail or will require repair or maintenance. The District is not liable for loss of or damage to student work-product caused by system failures, server crashes, or the District's performance of monitoring, maintenance or repair functions related to its computer systems or other electronic resources.

Legal Reference:

Education Code sections 35160 and 35160.1

Penal Code sections 313 and 502

18 U.S.C. section 1460

18 U.S.C. section 2246

18 U.S.C. sections 2252

20 U.S.C. section 6777 (Section 2441 of the No Child Left Behind Act of 2001)

47 U.S.C. section 254 (Neighborhood Children's Internet Protection Act)

New York v. Ferber (1982) 458 U.S. 747

Miller v. California (1973) 413 U.S. 15

Date Policy Adopted By the Board: March 20, 2002

Dates Policy Revised By The Board: January 13, 2005; June 5, 2008; July 18, 2013