



SAN YSIDRO SCHOOL DISTRICT

All Personnel

BP 4040(a)

EMPLOYEE USE OF TECHNOLOGY

The Governing Board recognizes that technological resources can enhance employee performance by improving access to and exchange of information, offering effective tools to assist in providing a quality instructional program, and facilitating district and school operations. The Board expects all employees to learn to use the available technological resources that will assist them in the performance of their job responsibilities. As needed, employees shall receive training in the appropriate use of these resources.

(cf. 0440 - District Technology Plan)
(cf. 1113 - District and School Web Sites)
(cf. 4032 - Reasonable Accommodation)
(cf. 4131 - Staff Development)
(cf. 4231 - Staff Development)
(cf. 4331 - Staff Development)
(cf. 6162.7 - Use of Technology in Instruction)
(cf. 6163.4 - Student Use of Technology)

Employees shall be responsible for the appropriate use of technology and shall use the district's technological resources only for purposes related to their employment. Such use is a privilege which may be revoked at any time.

(cf. 4119.25/4219.25/4319.25 - Political Activities of Employees)

Employees should be aware that computer files and communications over electronic networks, including e-mail and voice mail, are not private. These technologies shall not be used to transmit confidential information about students, employees or district operations without authority.

The Superintendent or designee shall ensure that all district computers with Internet access have a technology protection measure that prevents access to visual depictions that are obscene or child pornography, and that the operation of such measures is enforced. The Superintendent or designee may disable the technology protection measure during use by an adult to enable access for bona fide research or other lawful purpose. (20 USC 7001; 47 USC 254)

To ensure proper use of the system, the Superintendent or designee may monitor the district's technological resources, including e-mail and voice mail systems, at any time without advance notice or consent. If passwords are used, they must be known to the Superintendent or designee so that he/she may have system access.

The Superintendent or designee shall establish administrative regulations which outline employee obligations and responsibilities related to the use of district technology. He/she also may establish guidelines and limits on the use of technological resources. Inappropriate

use shall result in a cancellation of the employee's user privileges, disciplinary action and/or legal action in accordance with law, Board policy and administrative regulations.

BP 4040(b)

EMPLOYEE USE OF TECHNOLOGY (continued)

(cf. 4118 - Suspension/Disciplinary Action)

(cf. 4218 - Dismissal/Suspension/Disciplinary Action)

The Superintendent or designee shall provide copies of related policies, regulations and guidelines to all employees who use the district's technological resources. Employees shall be asked to acknowledge in writing that they have read and understood these policies, regulations and guidelines.

(cf. 4112.9/4212.9/4312.9 - Employee Notifications)

In the event that the use of an electronic resource affects the working conditions of one or more employees, the Superintendent or designee shall notify the employees' exclusive representative.

(cf. 4143/4243 - Negotiations/Consultation)

Legal Reference:

EDUCATION CODE

51870-51874 *Education technology*

GOVERNMENT CODE

3543.1 *Rights of employee organizations*

PENAL CODE

502 *Computer crimes, remedies*

632 *Eavesdropping on or recording confidential communications*

UNITED STATES CODE, TITLE 20

6801-6979 *Technology for Education Act*

7001 *Internet safety policy and technology protection measures, Title III funds*

UNITED STATES CODE, TITLE 47

254 *Universal service discounts (E-rate)*

CODE OF FEDERAL REGULATIONS, TITLE 47

54.520 *Internet safety policy and technology protection measures, E-rate discounts*

Management Resources:

CDE PUBLICATIONS

K-12 Network Technology Planning Guide: Building the Future, 1994

CDE PROGRAM ADVISORIES

1223.94 *Acceptable Use of Electronic Information Resources*

WEB SITES

CDE: <http://www.cde.ca.gov>

CSBA: <http://www.csba.org>

Federal Communications Commission: <http://www.fcc.gov>

U.S. Department of Education: <http://www.ed.gov>

American Library Association: <http://www.ala.org>

Policy
adopted: November 8, 2001
All Personnel

SAN YSIDRO SCHOOL DISTRICT
San Ysidro, California
AR 4040(a)

EMPLOYEE USE OF TECHNOLOGY

User Obligations and Responsibilities

Employees are authorized to use the District's on-line services and computers in accordance with user obligations and responsibilities specified below:

1. The employee in whose name an on-line services account is issued, is responsible for its proper use at all times. Users shall keep personal account numbers, home addresses and telephone numbers private. They shall use the system only under their own account number.
2. Employees shall use the system only for purposes related to their employment with the district. Commercial and political and/or personal use of the system is strictly prohibited. The district reserves the right to monitor any on-line communications for improper use.
3. Users shall not use the system to promote unethical practices or any activity prohibited by law or district policy. Users shall not send or request messages or documents that are inconsistent with school or district policies, guidelines, or codes of conduct.
4. Users shall not transmit material that is threatening, obscene, disruptive or sexually explicit, or that could be construed as harassment or disparagement of others based on their race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs.
5. Copyrighted material may not be placed on the system without the author's permission or pursuant to a valid license agreement. Users may download copyrighted material for their own use only and only in accordance with copyright laws and district procedures.
6. Vandalism will result in the cancellation of user privileges. Vandalism includes intentionally uploading, downloading or creating computer viruses and/or malicious attempts to harm or destroy district equipment or materials or the data of any other user.
7. Users shall not read other users' mail or files; they shall not attempt to interfere with other users' ability to send or receive electronic mail, nor shall they attempt to read, delete, copy, modify or forge other users' mail. Users shall not attempt to forge E-mail messages, or use an account owned by another user without written permission from that individual.

8. Users shall not use the network or equipment for commercial or financial gain or fraud.

AR 4040(b)

EMPLOYEE USE OF TECHNOLOGY (continued)

9. Users shall not gain or seek to gain unauthorized access to resources or entities.
10. Users shall not use the system to intentionally disrupt network traffic or crash the network and connected systems, or to degrade or disrupt equipment or system performance.
11. Users shall not possess any data which might be considered a violation of these rules in paper, magnetic (disk), or any other form.
12. Users shall report any misuse of the network to the immediate supervisor or designee.
13. Teacher assignments on the Internet should be age appropriate, and teachers must always thoroughly check out sites to which they direct students.
14. The district makes no warranties of any kind, whether express or implied, for the Internet or computer service it is providing. The district will not be responsible for any damages users suffer. This includes loss of data resulting from delays, non-deliveries, misdeliveries, or service interruptions caused by others negligence or the user's errors or omission. Use of any information obtained via the Internet is at the user's risk. The district specifically denies any responsibility for the accuracy or quality of information obtained through the Internet service.
15. Security on any computer is a high priority, especially when the system involves many users. If a user identifies a security problem on the Internet, he/she must notify the Director of the Information Management Services. Users shall not demonstrate the problem to the other users. Attempts to log on to the Internet or any district computer as a system administrator will result in cancellation of user privileges. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the Internet.
16. The district declares that a violation of this policy may be just cause for taking disciplinary action, revoking networking privileges and/or initiating legal action. The use of the Internet is a privilege, and unacceptable use will result in a cancellation of those privileges.

Viruses and Software

For the protection of the network, no user is allowed to use infected floppy disks, nor to introduce any virus or other computer program for the purpose of interfering with the normal

operation of the computer system. Employees shall not create, distribute, or purposely activate a computer virus or worm. Persons responsible for a computer becoming infected with viruses or worms, will be held financially and personally liable for any damage caused by such introduction of a virus, worm or other destructive program.

AR 4040(c)

EMPLOYEE USE OF TECHNOLOGY (continued)

Employees shall not use software for which they have a valid license, but for which the district does not have a valid license, or district computers unless they have received prior approval pursuant to guidelines established by the Superintendent or his/her designee. Such guidelines shall require that employees use software only in conformity with applicable license agreements and copyright law. Employees are strictly prohibited from installing or loading software onto district computers unless and until approval is received.

Violation of this policy and guidelines may be just cause for taking discipline action, revoking networking privileges and/or initiating legal actions.

Regulation
approved: November 8, 2001

SAN YSIDRO SCHOOL DISTRICT
San Ysidro, California