

# **EMPLOYEE USE OF TECHNOLOGY AND EMPLOYEE COMMUNICATION**

## **Policy of the Board of Education**

The governing board recognizes that effective employee communication skills are essential to obtaining district goals. The governing board intends for all employees to be effective communicators. Employees should present clear, effective messages reflecting positively on the organization and demonstrating a high degree of professionalism. These expectancies apply to all types of communication including contacts over the phone, by electronic mail, letters, brochures, slide shows, videos, and any other type of medium. Monitoring by authorized administrators of employee e-mail, Internet use, and other employee use of District equipment to include use of the District electronic system(s) is viewed as necessary to manage the District's electronic risks.

The governing board also recognizes that technology 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 operations. The board expects all employees to learn to use the available electronic resources that will assist them in their jobs. As needed, staff shall receive training in the appropriate use of these resources.

Employee use of district resources is a privilege which may be revoked at any time. Employees shall have no expectation of privacy in their use of the district's electronic system(s) including, but not limited to, use of: (a) computer records, (b) electronic mail (e-mail), (c) Internet access, (d) electronic bulletin board systems, (e) interactive messaging services, (f) interactive chat services, Internet Relay Chat or Web-based chat systems, (g) Usenet newsgroups, (h) the World Wide Web, (i) electronic mailing lists, (j) use of local area networks; (k) intranets, (l) voice mail and (m) other communications transmitted over a District electronic system or stored/recorded at any point in the District-provided systems. Technology shall not be used to transmit confidential information about students, employees, or district affairs without authority to do so and unless effective safeguards have been established. The superintendent or designee will protect against unauthorized disclosures by instituting procedures to: (a) electronically block unauthorized persons from accessing protected files such as pupil records and (b) require employees to reasonably protect all confidential files.

(cf. BP 300.49 Unauthorized Release of Privileged/Confidential Information)

(cf. BP 100.51 Disclosure of Confidential/Privileged Information)

(cf. BP 605.7 Pupil Records)

# EMPLOYEE USE OF TECHNOLOGY AND EMPLOYEE COMMUNICATION

## Policy of the Board of Education

While using District equipment (e.g., computer), completing work for the District, or at any time when an employee or independent contractor is supposed to be working for the District the following conduct is prohibited: (a) obscenity; (b) sexually explicit messages; (c) pornography, including child pornography; (d) threats; (e) fighting words; (f) intimidation; (g) libel, defamation, and slander; (h) harassment of any kind, including harassment on the basis of: (1) race, (2) color; (3) ancestry; (4) gender, (5) religion, (6) housing status, (7) economic status, (8) marital or parental status; (9) citizenship status or nationality, (10) age, (11) illness, (12) physical disability, (13) mental disability, (14) sexual orientation; (i) humor or jokes that are intended to offend, harass, or intimidate or are likely to offend, harass or intimidate a reasonable person; (j) chain letters; (k) multilevel marketing opportunities; (l) business opportunity ventures; (m) investments; (n) pyramid schemes; (o) unsolicited e-mail and “spamming” (Spam is unsolicited commercial bulk e-mail); (p) violating any applicable laws; (q) violating the privacy of any individual; (r) violating the property rights of any other person, business or organization; (s) unauthorized copying or transmission of: (1) text, (2) other communications, (3) computer software, (4) photographs, (5) video images, (6) graphics, (7) music, or (8) sound recordings.

(cf. BP 300.27 Nondiscrimination)  
(cf. BP 400.34 Use of Copyright Materials)  
(cf. BP 500.38 Sexual Harassment)

E-mail use and Internet access are restricted to appropriate business-related use and may not be used for the benefit of any other business or organization. With respect to *prohibited* communications listed above, employees are not authorized to take any of the following actions: (a) transmitting; (b) uploading; (c) downloading; (d) cutting, pasting, and copying; (e) forwarding or retransmitting; (f) attaching to e-mail messages; (g) attaching to chat messages; (h) posting in a public access area; (i) printing; (j) saving to disk or other storage medium; and (k) sending by fax. Playing Internet or Web-based games during work hours is prohibited.

The Superintendent or designee shall ensure that all district equipment with Internet access have a technology protection measure(s), to include measures that prevent access to visual depictions that are obscene or contain child pornography content. Technology protection measures may include, but are not necessarily limited to: (a) installation of firewalls with secure passwords; (b) maintaining proper configuration of firewalls, routers, and other network components critical to security; (c) encrypted electronic transmission; (d) placing security duties in the role of the network administrator(s); (e) periodically assessing computer system security and correcting any

# **EMPLOYEE USE OF TECHNOLOGY AND EMPLOYEE COMMUNICATION**

## **Policy of the Board of Education**

problems identified; (f) limiting physical access to rooms in which computers are kept; and (g) educating employees about how individuals wishing to penetrate the district's system(s) engage in intelligence gathering and "hack" into systems.

The operation of protection measures will be properly enforced by the Superintendent or designee. The Superintendent or designee may disable the technology protection measure(s) during use by an adult to enable access for bona fide research or other lawful purpose (20 United States Code 7001; 47 United States Code 254).

To help ensure proper use of the electronic system(s), the Superintendent or designee may monitor any of the district's technological resources, including e-mail and voice-mail systems, at any time without advance notice or consent. When passwords are used by an employee, the passwords are made known to the Superintendent or designee so that he/she may have system and equipment access.

The Superintendent or designee shall establish administrative regulations which outline additional 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 of district resources may 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.

### **Legal Reference:**

#### **EDUCATION CODE**

51870-51874 Education technology

#### **PENAL CODE**

502 Computer crimes, remedies

632 Eavesdropping on or recording confidential communications

#### **UNITED STATES CODE, TITLE 18**

1702 Obstruction of correspondence

2510-2701 Electronic Communications Privacy Act

#### **UNITED STATES CODE, TITLE 20**

6801 – 6979 Technology for Education Act of 1994

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

# **EMPLOYEE USE OF TECHNOLOGY AND EMPLOYEE COMMUNICATION**

## **Policy of the Board of Education**

### **Other References:**

**Alcala v. Calderon WL446234 N.D. Cal. 1997**

Author. (June 1999). Positive Communications and Stylebook. Bakersfield, California: Office of Kern County Superintendent of Schools.

Bohach v. City of Reno 932 F.Supp. 1232 (D. Nev. 1996)

Federal Bureau of Investigation Advisory. Retrieved January 16, 2002 from  
<http://www.fbi.gov/pressrel/pressrel01/mail3.pdf>

Flynn, N. (2001). The ePolicy Handbook: Designing and Implementing Effective E-Mail, Internet, and Software Policies. New York: American Management Association.

Imparl, S.D. (1998). Internet Law: The Complete Guide. North Vancouver, B.C.: Specialty Technical Publishers, Inc.

Security of the Mail. United States Postal Service, Retrieved January 16, 2002 from  
<http://www.usps.com/news/2001/press/serviceupdates.htm>

Revision Adopted (Entire Section) March 22, 1985, November 9, 1999

Revision Adopted April 23, 2002

# EMPLOYEE USE OF TECHNOLOGY AND EMPLOYEE COMMUNICATION

## Administrative Regulation

### Telephone User Obligations and Responsibilities

The standards for telephone communications by district employees are as follows.

1. If an employee transfers a telephone call, he or she gives the caller the name and phone number of the person he/she is being transferred to and remains on the line until the connecting party is reached. If the transfer can not be completed, the employee offers to take a message or, when appropriate, to transfer the caller to another employee in the department or to voice mail.
2. The principal/designee or department administrator shall ensure that when incoming calls are forwarded, the person(s) receiving these forwarded calls is aware of the arrangement. It is generally appropriate to have pre-agreed upon procedures to appropriately respond to forwarded calls.
3. When taking a message, the employee writes down the: (a) name of caller, (b) phone number where caller can be reached, (c) reason (nature and urgency) of the call, (d) date and time of the call, and (e) name of the person taking the call. Written messages should be made accessible to the appropriate employee within thirty minutes after receiving such a message.
4. The principal/designee or department administrator may authorize the use of voice mail to initially answer a call. The caller receives a notice of how a responsible employee may be contacted by the caller in an emergency (e.g., notices include another telephone number, an opportunity to connect to a live person, a beeper number, cell phone number). An example of an appropriate voice mail message for such conditions include: "You have reached the desk of John Doe in the Special Services Department. Staff will not be available between the hours of 11:00 a.m. and 1:00 p.m. today September 29. Please leave a voice mail message. If there is an emergency, please call Sally Jones on her cell phone at 000-0000."
5. Responses to callers and voice mail messages will not make reference to vacations, lunch hours, medical or personal appointments, breaks or give other explanation of why the employee is away. Examples of appropriate voice mail messages include: "I will be away

# EMPLOYEE USE OF TECHNOLOGY AND EMPLOYEE COMMUNICATION

## Administrative Regulation

from the office May 11. I will be checking my messages. Should you need immediate assistance, please contact (name of person and title) at extension (number).” OR “I will be away from the office from May 17 through June 10. Please contact (name of person and title) at extension (number) for further assistance.”

6. Voice mail messages left for callers and voice mail messages an employee-caller leaves for others to hear will be brief and clear.
7. When a voice mail message refers the caller to another employee for assistance, the employee who will provide assistance will receive notice before the voice mail message is recorded for use on the telephone system.
8. Unless the superintendent or designee determines an emergency exists, district employees will not use the following phone features: (a) “override,” whereby a user bridges into a busy connection, (b) “do not disturb,” (DND) whereby a telephone station is programmed to show busy, (c) “voice call” or “internal zone paging” whereby a user’s call goes direct to the called parties’ built-in speaker, or (d) “privacy release” whereby a caller enters the conversation of a person already engaged in communication unless the person engaged in the conversation explicitly authorizes the conversation entry.

Nothing in these administrative regulations requires an employee to continue conversing with a caller who uses inappropriate communication including, but not necessarily limited to: threats against the employee, profane or obscene language, unethical or illegal solicitation, sexually explicit, racist or sexist comments. The employee may provide a warning to the other person that such conduct is inappropriate and may lead to termination of the conversation.

Principals and department heads shall inform their respective staffs that telephones are primarily a medium for conducting school business. Principals, directors and superintendents may use approved district procedures to make long distance telephone calls in connection with school business. Teachers shall be called from classrooms to answer telephone calls only under urgent circumstances.

## **Cellular Phone Use**

As part of the district’s comprehensive safety planning and to promote effective, timely communication, the district may establish an account and provide a cellular phone to an employee. District cellular phones may not be used for private business unless the district is reimbursed for private business expenses by the employee.

# EMPLOYEE USE OF TECHNOLOGY AND EMPLOYEE COMMUNICATION

## Administrative Regulation

### **On-Line User Obligations and Responsibilities**

Employees are authorized to use the district's on-line services in accordance with Governing Board policy and the user obligations and responsibilities specified in board policy and listed below.

1. The employee in whose name the district on-line services access account is issued is responsible for its proper use at all times. Employees shall keep personal account information, home addresses and telephone numbers private. They shall use the district system only under their assigned district access account.
2. Employees shall use district resources (e.g., a computer) only for purposes related to their employment with the district. Commercial, political and/or personal use of the district resources is strictly prohibited. The district reserves the right to monitor any on-line communications for improper use. Information obtained or manipulated (e.g., copied, attached, uploaded, stored, viewed, transmitted) using district resources is not private.
3. Employees shall not use any district resources to promote unethical practices or any activity prohibited by law, Board policy, or administrative regulations (e.g., no soliciting, advertising for private gain, disclosure of confidential information).
4. Employees shall not transmit, access, post, submit, publish, or display harmful matter or material that is threatening, obscene, disruptive or sexually explicit, or that could be construed as harassment or disparagement of others based on their race/ethnicity, national origin, sex, sexual orientation, age, disability, religion or political beliefs.
5. Copyrighted material (e.g., computer software) may not be placed on the system without the author's permission. Employees may download copyrighted material for their own use only and only in accordance with copyright laws.
6. Employees shall not intentionally upload, download, or create computer viruses and/or maliciously attempt to harm, alter or destroy district equipment or materials or the data of any other user, including so-call "hacking." Such vandalism will result in the cancellation of employee privileges

## EMPLOYEE USE OF TECHNOLOGY AND EMPLOYEE COMMUNICATION

### Administrative Regulation

7. Without authority, employees shall not read other employee's mail or files. Employees shall not attempt to interfere with other employees' ability to send or receive electronic mail, nor shall they attempt to delete, copy, modify or forge other employees' mail.
8. Employees will comply with all applicable rules, laws, and policies.

### **Hard Copy Mail**

Employees do not direct personal mail to be delivered to any District facility. District mailboxes may not be used to distribute unauthorized mail. Additionally, "junk mail" is defined as mail received by the District, but not directed to a specific person or department (18 United States Code 1702). Junk mail will be safely discarded rather than distributed.

"Suspicious mail" includes, but is not necessarily limited to: (a) mail that is handwritten and has no return address or bears a return address that cannot be confirmed; (b) mail that is lopsided or lumpy in appearance; (c) mail sealed with excessive amounts of tape and containing no return address; (d) mail marked with restrictive endorsements such as "personal" or "confidential;" (e) mail with: (1) protruding wire, (2) a strange odor, (3) oily stains, discolorations, or crystallization in the wrapper, (4) misspelled words, badly typed or written; and (f) items possibly mailed from a foreign country (United States Postal Service, 2002 & Federal Bureau of Investigation, 2002).

Suspicious mail may lead an employee to identify a threat. Experts recommend that individuals not handle a letter or package suspected of being contaminated. Persons are not to shake, bump, or sniff mail that presents a threat. In the case of a suspected bomb, the facility containing the mail is immediately evacuated. If a radiological danger may exist, employees are to limit exposure to the mail item, refrain from handling the item, and to shield themselves from the object. If a biological or chemical danger may exist, the person(s) is to refrain from handling the item, to isolate themselves from the item, and to wash their hands with soap and water.

Employees are to notify a responsible administrator and, when appropriate, contact law enforcement should a threat be identified (United States Postal Service, 2002 & Federal Bureau of Investigation, 2002). *If the delivery of mail to an employee will be significantly delayed, the employee will receive a notice of the delay.*

# EMPLOYEE USE OF TECHNOLOGY AND EMPLOYEE COMMUNICATION

## Administrative Regulation

(cf. BP 300.9 Safety and Civil Defense Disaster Preparedness Plan)  
(cf. BP 300.36 Crisis Intervention)

### **Electronic Mail**

E-mail, file attachments and other uses of the District's electronic system(s) commonly creates a process by which communications are recorded and District business decisions are documented. Written documents end up stored in electronic mailboxes and on hard drives, file servers, and backup tapes. Some e-mail documents may meet the definition of a public record and be subject to disclosure to persons other than employees. E-mail, attachments, and other electronic communication must be businesslike and free of unnecessary, prohibited and inappropriate language. The employee should purge e-messages soon after receipt.

(cf. BP 300.22 District Records)

Employees using any form of electronic mail (e-mail) originating or received on any district computer, electronic system or medium will follow these standards: (a) employees do not "reply to all senders" unless the e-mail is specifically intended as a reply to everyone on a distribution list, (b) employees avoid replying to an e-mail message by re-sending the entire original message, and (c) if a file is attached to an e-mail sent by an employee, the sender will notify the intended recipient of: (1) the number of attachments, (2) type of file(s) and (3) the program version needed to use the file. Employees are prohibited from the following:

1. Whether the letter originates internally or externally, starting or forwarding any "chain letters." Sending notices to other users about potential virus threats. All information on virus threats will be sent by the superintendent or designee only after verifying a virus does exist and what steps employees should take.
2. Sending broadcast messages to all users on the e-mail system without permission of the superintendent or designee.
3. Storing and forwarding large files, e.g., over one megabyte, over the e-mail system.
4. All additional prohibited conduct is listed in the board policy accompanying this Administrative Regulation and related policies.

# **EMPLOYEE USE OF TECHNOLOGY AND EMPLOYEE COMMUNICATION**

## **Administrative Regulation**

### **Video, Television, and Multimedia Productions**

District employees shall comply with the standards below when producing presentations that may be viewed by others to include, but not necessarily limited to: live and taped television productions, video, slide shows, interactive CD-ROMs, digital presentations on web sites, Power Point, or similar presentations.

Information at the beginning of the program is optional, but should include brief opening credits and a date of publication. Somewhere in the program or presentation, the Bakersfield City School District and the department/school responsible for the content of the production will be identified.

Web sites developed by employees for departments and divisions must have been reviewed by the superintendent or designee before they are posted on the Internet.

### **Security**

Employees are responsible for the safekeeping of all equipment (e.g., computer, phone) and any facility (e.g., classroom) assigned to the employee. Each employee assigned district property shall secure the property to reduce the likelihood of improper access, damage, loss, or criminal activity. Employees should avoid an open, online computer by requiring a password to be re-entered or shutting off the computer if the employee plans to be away from his or her desk. Passwords should be kept safeguarded, however a current record should be kept of all passwords by the administrator overseeing the work of the employee. Passwords are the property of the District, not the individual employee.

If there is a suspicion or evidence of district property being accessed or used improperly, the employee assigned the equipment or facility or other employee shall promptly make a report to the responsible administrator.

(cf. BP 300.42 Campus Security)  
(cf. BP 300.44 School Safety Plan)  
(cf. BP 800.7 Illegal Entry – Damage – Theft)

# EMPLOYEE USE OF TECHNOLOGY AND EMPLOYEE COMMUNICATION

## Administrative Regulation

### Disciplinary Action

Employees violating district policy and administrative regulations may be subject to disciplinary action, revocation of the employee access account and legal action as appropriate. Each employee has a responsibility to report abuses of district resources.

(cf. BP 400.43 Student Use of Technology/Acceptable Use)

### Legal Reference:

#### EDUCATION CODE

51870-51874 Education technology

#### PENAL CODE

502 Computer crimes, remedies

632 Eavesdropping on or recording confidential communications

#### UNITED STATES CODE, TITLE 18

1702 Obstruction of correspondence

2510-2701 Electronic Communications Privacy Act

#### UNITED STATES CODE, TITLE 20

6801 – 6979 Technology for Education Act of 1994

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

### Other References:

Alcala v. Calderon WL446234 N.D. Cal. 1997

Author. (June 1999). Positive Communications and Stylebook. Bakersfield, California: Office of Kern County Superintendent of Schools.

Bohach v. City of Reno 932 F.Supp. 1232 (D. Nev. 1996)

Flynn, N. (2001). The ePolicy Handbook: Designing and Implementing Effective E-Mail, Internet, and Software Policies. New York: American Management Association.

Imparl, S.D. (1998). Internet Law: The Complete Guide. North Vancouver, B.C.: Specialty Technical Publishers, Inc.

Revision Adopted (Entire Section) March 26, 1985

Revision Adopted November 26, 1991, November 9, 1999

Revision Adopted April 23, 2002

Revision Adopted January 27, 2004