Board Policy
District Records

BP 3580
Business and Noninstructional Operations

The Governing Board recognizes the importance of securing and retaining district documents. The Superintendent or designee shall ensure that district records are developed, maintained, and disposed of in accordance with law, Board policy, and administrative regulation.

The Board recognizes that the use of email and other electronic communication in the workplace has increased tremendously, raising issues with respect to communication, creation of information and systems, and retrieval and storage of electronic records. The Board further acknowledges the District's responsibility to make records available to the public, with certain exceptions. Accordingly, the Board directs that all electronic records of this District be maintained, safeguarded and disclosed in full compliance with the requirements of law. This includes records created, sent or received using District computers and communications systems or using the *personal* electronic devices or accounts of District employees and officials, if substantive District business issues are discussed.

Access to the District's computers and the District's information and communications systems and equipment is controlled and administered by the District's information technology department. The District has the right to disclose, as permitted or required by applicable law, any communications or records, or copies of communications or records stored for any period of time in or by the District's information and communications system or equipment, and all communications constituting District-related business in the personal accounts of District employees and officials. Communications constituting District-related business are those communications that relate in a substantive way to the conduct of the District's business. Communications that are primarily personal in nature or that contain no more than incidental mentions of the District's business may not constitute District-related business communications. The District may monitor or access employee communications made using the District's information and communication systems and equipment, and employees should have no expectation of privacy when using the District's information and communication systems and equipment. When passwords are used, they must be known to the Superintendent or designee so that he/she may have system access.

(cf. 1340 - Access to District Records)
(cf. 3440 - Inventories)
(cf. 4112.6/4212.6/4312.6 - Personnel Files)
(cf. 5125 - Student Records)

The Superintendent or designee shall consult with district legal counsel, site administrators, district information technology staff, personnel department staff, and others as necessary to develop a secure document management system that provides for the storage, retrieval, archiving, and destruction of district documents, including electronically stored information such as email. This document management system shall be designed to comply with state and federal laws regarding security of records, record retention and destruction, response to "litigation hold" discovery requests, and the recovery of records in the event of a disaster or emergency.

(cf. 0440 - District Technology Plan)
(cf. 3516 - Emergencies and Disaster Preparedness Plan)
(cf. 4040 - Employee Use of Technology)
(cf. 9011 - Board Member Electronic Communications)

The Superintendent or designee shall ensure the confidentiality of records as required by law and shall establish regulations to safeguard data against damage, loss, or theft.

(cf. 5125.1 - Release of Directory Information)

The Superintendent or designee shall ensure that employees receive information about the district's document management system, including retention and confidentiality requirements and an employee's obligations in the event of a litigation hold established on the advice of legal counsel.

(cf. 4131 - Staff Development)
(cf. 4231 - Staff Development)
(cf. 4331 - Staff Development)

If the district discovers or is notified that a breach of security of district records containing unencrypted personal information has occurred, the Superintendent or designee shall notify every individual whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Personal information includes, but is not limited to, a social security number, driver's license or identification card number, medical information, health insurance information, or an account number in combination with an access code or password that would permit access to a financial account. (Civil Code 1798.29)

The Superintendent or designee shall provide the notice in a timely manner either in writing or electronically, unless otherwise provided in law. The notice shall include the material specified in Civil Code 1798.29, be formatted as required, and be distributed in a timely manner, consistent with the legitimate needs of law enforcement to conduct an uncompromised investigation or any measures necessary to determine the scope of the breach and restore reasonable integrity of the data system. (Civil Code 1798.29)

(cf. 1112 - Media Relations)
(cf. 1113 - District and School Web Sites)
(cf. 4112.9/4212.9/4312.9 - Employee Notifications) (cf.
5145.6 - Parental Notifications)

Safe at Home Program

District public records shall not include the actual addresses of students, parents/guardians, or employees when a substitute address is designated by the Secretary of State pursuant to the Safe at Home program. (Government Code 6206, 6207)

When a substitute address card is provided pursuant to this program, the confidential, actual address may be used only to establish district residency requirements for enrollment and for school emergency purposes.

(cf. 5111.1 - District Residency)
(cf. 5141 - Health Care and Emergencies)

Legal Reference: EDUCATION
CODE
35145 Public meetings
35163 Official actions, minutes and journal
35250-35255 Records and reports
44031 Personnel file contents and inspection
49065 Reasonable charge for transcripts 49069
Absolute right to access
CIVIL CODE
1798.29 Breach of security involving personal information CODE
OF CIVIL PROCEDURE
1985.8 Electronic Discovery Act
2031.010-2031.060 Civil Discovery Act, scope of discovery demand
2031.210-2031.320 Civil Discovery Act, response to inspection demand
GOVERNMENT CODE
6205-6210 Confidentiality of addresses for victims of domestic violence, sexual assault or stalking
6252-6265 Inspection of public records
12946 Retention of employment applications and records for two years
PENAL CODE
11170 Retention of child abuse reports
CODE OF REGULATIONS, TITLE 5
430 Individual student records; definition
432 Varieties of student records
16020-16022 Records, general provisions
16023-16027 Retention of records
UNITED STATES CODE, TITLE 20
1232g Family Educational Rights and Privacy Act CODE
OF FEDERAL REGULATIONS, TITLE 34
99.1-99.8 Family Educational Rights and Privacy Act

Management Resources:
WEB SITES
California Secretary of State: http://www.sos.ca.gov/safeathome