

**DISTRICT RECORDS**

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.

*(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)

**DISTRICT RECORDS** (continued)

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: (see next page)*

**DISTRICT RECORDS** (continued)

*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>*

**DISTRICT RECORDS**

**Classification of Records**

*Records* means all records, maps, books, papers, and documents of a school district required by law to be prepared or retained as necessary or convenient to the discharge of official duty. (5 CCR 16020)

*(cf. 1340 - Access to District Records)*

Before January 1, the Superintendent or designee shall review the prior year's records and shall classify them as either a Class 1 (Permanent), Class 2 (Optional), or Class 3 (Disposable) record. (5 CCR 16022)

*Records of continuing nature* (active and useful for administrative, legal, fiscal, or other purposes over a period of years) shall not be classified until such usefulness has ceased. (5 CCR 16022)

An inventory of equipment shall be a continuing record and shall not be classified until the inventory is superseded or until the equipment is removed from district ownership. (5 CCR 16022)

*(cf. 3440 - Inventories)*

A student's cumulative record is a continuing record until the student ceases to be enrolled in the district. (5 CCR 16022)

*(cf. 5125 - Student Records)*

When an electronic or photographed copy of a Class 1 (Permanent) record has been made, the copy may be classified as Class 1 (Permanent) and the original classified as either Class 2 (Optional) or Class 3 (Disposable). However, no original record that is basic to any required audit may be destroyed prior to the second July 1st succeeding the completion of the audit. (Education Code 35254)

**Class 1 - Permanent Records**

The original of each of the following records, or one exact copy of it when the original is required by law to be filed with another agency, is a Class 1 (Permanent) record and shall be retained indefinitely unless microfilmed in accordance with 5 CCR 16022: (5 CCR 16023)

1. Annual Reports
  - a. Official budget
  - b. Financial reports of all funds, including cafeteria and student body funds

**DISTRICT RECORDS** (continued)

- c. Audit of all funds
- d. Average daily attendance, including Period 1 and Period 2 reports
- e. Other major annual reports, including:
  - (1) Those containing information relating to property, activities, financial condition, or transactions
  - (2) Those declared by Governing Board minutes to be permanent

*(cf. 3100 - Budget)*

*(cf. 3452 - Student Activity Funds)*

*(cf. 3460 - Financial Reports and Accountability)*

*(cf. 3551 - Food Service Operations/Cafeteria Fund)*

2. Official Actions

- a. Minutes of the Board or Board committees, including the text of rules, regulations, policies, or resolutions included by reference only
- b. The call for and the result of any elections called, conducted, or canvassed by the Board
- c. Records transmitted by another agency pertaining to its action with respect to district reorganization

*(cf. 7214 - General Obligation Bonds)*

*(cf. 9324 - Minutes and Recordings)*

3. Personnel Records

Class 1 (Permanent) records include all detailed records relating to employment; assignment; amounts and dates of service rendered; termination or dismissal of an employee in any position; sick leave record; rate of compensation, salaries, or wages paid; and deductions or withholdings made and the person or agency to whom such amounts were paid. In lieu of the detailed records, a complete proven summary payroll record for each employee containing the same data may be classified as a Class 1 (Permanent) record and the detailed records may then be classified as Class 3 (Disposable) records.

Information of a derogatory nature as defined in Education Code 44031 shall be retained as a Class 1 (Permanent) record only when the time for filing a grievance has passed or the document has been sustained by the grievance process.

## **DISTRICT RECORDS** (continued)

*(cf. 4112.5/4212.5/4312.5 - Criminal Record Check)*

*(cf. 4112.6/4212.6/4312.6 - Personnel Files)*

### 4. Student Records

The records of enrollment and scholarship for each student required by 5 CCR 432 and all records pertaining to any accident or injury involving a minor for which a claim for damages had been filed as required by law shall be classified as Class 1 (Permanent) records. These include any related policy of liability insurance, except that these records cease to be Class 1 (Permanent) records one year after the claim has been settled or the statute of limitations has expired.

*(cf. 5111.1 - District Residency)*

*(cf. 5141 - Health Care and Emergencies)*

*(cf. 5143 - Insurance)*

### 5. Property Records

Class 1 (Permanent) records include all detailed records relating to land, buildings, and equipment. In lieu of detailed records, a complete property ledger may be classified as a Class 1 (Permanent) record. The detailed records may then be classified as Class 3 (Disposable) records if the property ledger includes all fixed assets; an equipment inventory; and, for each piece of property, the date of acquisition, name of previous owner, a legal description, amount paid, and comparable data if the unit is disposed of.

*(cf. 3280 - Sale or Lease of District-Owned Real Property)*

## **Class 2 - Optional Records**

Any records considered temporarily worth keeping, but which are not Class 1 records, may be classified as Class 2 (Optional) records and shall be retained until reclassified as Class 3 (Disposable) records. If, by agreement of the Board and Superintendent or designee, classification of the prior year records has not been made before January 1 as specified in 5 CCR 16022, all records of the prior year may be classified as Class 2 (Optional) records pending further review and classification within one year. (5 CCR 16024)

## **Class 3 - Disposable Records**

All records not classified as Class 1 (Permanent) or as Class 2 (Optional) records shall be classified as Class 3 (Disposable) records. These include, but are not limited to, detailed records basic to audit, including those relating to attendance, average daily attendance, or business or financial transactions; detailed records used in preparing another report; teachers' registers if all information required by 5 CCR 432 is retained in other records or if the

## **DISTRICT RECORDS** (continued)

General Records pages are removed from the register and classified as Class 1 (Permanent) records; and periodic reports, including daily, weekly, and monthly reports, bulletins, and instructions. (5 CCR 16025)

All Class 3 (Disposable) records shall be destroyed during the third school year after the school year in which the records originated. In addition, Class 3 (Disposable) records shall not be destroyed until after the third school year following the completion of any legally required audit or the retention period required by any agency other than the State of California, whichever is later. A continuing record shall not be destroyed until the fourth year after it has been classified as a Class 3 (Disposable) record. (5 CCR 16026, 16027)

*(cf. 5113.2 - Work Permits)*

### **Electronically Stored Information**

All electronically stored information related to the conduct of district business, including information created, saved, sent, or received on a district employee's or Board member's personal account or device, shall be saved as an electronic file to a district-provided account or device and retained in accordance with the section "Classification of Records" above. Such information includes, but is not limited to, email, text messages, instant messages, computer files, and other electronic communications related to district business. In addition, when appropriate, the information may be printed and physically filed in a way that allows it to be easily retrieved when needed.

*(cf. 9012 - Board Member Electronic Communications)*

Employees shall be required to regularly purge their email accounts and district-issued computers, cell phones, and other communication devices of personal electronically stored information and other information unrelated to district business. The Superintendent or designee may check for appropriate use of any district-owned equipment at any time. Employees should have no expectation that any communications made using the district's information and communication systems and equipment are exempt from monitoring or access by the district.

*(cf. 4040 - Employee Use of Technology)*

Any person to whom a district-owned computer, cell phone, or other electronic communication device is provided shall be notified about the district's electronic information management system and, as necessary, provided training on the effective use of the device.

### **Retention of Electronic Records**

The Governing Board recognizes that the use of email and other electronic communication in the workplace has increased tremendously, raising issues with respect to communication,

**DISTRICT RECORDS** (continued)

creation of information and systems, and retrieval and storage of electronic records. The Governing Board further acknowledges the District's responsibility to make records available to the public, with certain exceptions. Accordingly, the Governing Board directs that all electronic records of the district be maintained, safeguarded and disclosed in full compliance with the requirements of the law.

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. 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.

District email accounts are not intended for permanent storage of district records. It is each employee's responsibility to save and/or file email that he or she receives and wishes thereafter to access, or that are district records and required to be retained by law. "District records" means all records, maps, books, papers, and documents prepared or retained as necessary or convenient to the discharge of official duty and includes any writing containing information related to the conduct of the public's business prepared, owned, used or retained by the district regardless of physical characteristics. Emails or other electronic records related to district business shall be either:

1. Saved to an electronic system other than the district email account.
2. Electronically archived, or
3. Printed on paper and filed as appropriate.

The district may access and, to the extent required by law, disclose any email received, sent, or stored in a district email account. The district may retain or dispose of an employee's email, whether an employee is currently or formerly employed by the district. It is presumed that district business emails will be stored in such manner by district employees on a regular basis, and therefore emails older than one year may be purged by the district's information technology department, unless such emails are relevant to litigation or anticipated litigation.