District Records

Adopted: 05/01/2007 **| Last Revised:** 08/04/2026 **| Last Reviewed**: 08/04/2026

The Board of Education 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 rule.

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.

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, which may be caused by cybersecurity breaches.

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 or California Public Records Act request established on the advice of legal counsel. Additionally, the Superintendent or designee shall ensure that employees receive information and training about cybersecurity, including ways to protect district records from breaches to the district's digital infrastructure.

If the district discovers or is notified that a breach of security of district records has resulted in the release of personal information, the Superintendent or designee shall notify every individual whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person, if that information was either unencrypted or encrypted under the circumstances specified in Civil Code 1798.29. "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.

The Superintendent or designee shall provide the notice 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.

If the district experiences a cyberattack that impacts more than 500 students or personnel, the Superintendent or designee shall report the cyberattack to the California Cybersecurity Integration Center.

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.

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.

Records containing a participant's confidential address information shall be kept in a confidential location and not shared with the public.

Policy Reference Disclaimer:
These references are not intended to be part of the policy itself, nor do they indicate the basis or authority for the Board to enact this policy. Instead, they are provided as additional resources for those interested in the subject matter of the policy.

Legal References:

STATE
CALIFORNIA CODE OF REGULATIONS
5 CCR 16020-16022 Records; general provisions
5 CCR 16023-16027 District records; retention and destruction
5 CCR 430-438 Individual student records
CIVIL CODE
1798.29 District records; breach of security
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
EDUCATION CODE
35145 Public meetings
35163 Official actions, minutes and journal
35252-35255 Records and reports
35266 Cybersecurity
44031 Personnel file contents and inspection
49065 Reasonable charge for transcripts
49069.7 Absolute right to access
GOVERNMENT CODE
11549.3 Office of Information Security
12946 Fair Employment and Housing Act: discrimination prohibited
6205-6210 Confidentiality of addresses for victims of domestic violence, sexual assault, stalking, human trafficking, child abduction, and elder or dependent adult abuse
6215-6216 Address confidentiality; reproductive health care providers, employees, volunteers, patients, and other individuals who face threats or violence
7920.000-7930.215 California Public Records Act
8586.5 Office of Emergency Services; California Cybersecurity Information Center
PENAL CODE
11170 Retention of child abuse reports
FEDERAL
UNITED STATES CODES
20 USC 1232g Family Educational Rights and Privacy Act (FERPA) of 1974
CODE OF FEDERAL REGULATIONS
34 CFR 99.1-99.8 Family Educational Rights and Privacy Act
MANAGEMENT RESOURCES
CALIFORNIA SECRETARY OF STATE PUBLICATION
Records Management Handbook
STATE ED. TECH. DIRECTORS ASSOCIATION PUBLICATION
Small Districts, Big Hurdles: Cybersecurity Support for Small, Rural, and Under-resourced School Districts, October 2023

WEBSITES

Safe at Home; Schools https://www.sos.ca.gov/registries/safe-home/schools#:~:text=Back%20to%20Top-,Verifying%20Enrollment,(916)%20653%2D1769

Federal Communications Commission, Schools and Libraries Cybersecurity Pilot Program https://www.fcc.gov/cybersecurity-pilot-program

Cybersecurity and Infrastructure Security Agency, Government Coordinating Councils https://www.cisa.gov/resources-tools/groups/government-coordinating-councils

California Office of Emergency Services https://www.caloes.ca.gov/

CSBA District and County Office of Education Legal Services https://legalservices.csba.org/

California Secretary of State http://www.sos.ca.gov/safeathome

---

Policy Adopted: 05/01/2007
Revised: 02/20/2018
Revised: 08/04/2026