



BUSINESS AND NONINSTRUCTIONAL OPERATIONS

BOARD POLICY – SBCEO RECORDS

BP 3580

The Santa Barbara County Board of Education and the County Superintendent of Schools recognize the importance of securing and retaining SBCEO documents. The Superintendent or designee shall ensure that SBCEO records are developed, maintained, and disposed of in accordance with law, Board policy, and administrative regulation.

The Superintendent or designee shall consult with SBCEO legal counsel, site administrators, SBCEO 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 SBCEO 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, including damage, loss, or theft which may be caused by cybersecurity breaches.

The Superintendent or designee shall ensure that employees receive information about the SBCEO’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 SBCEO records from breaches to the SBCEO’s digital infrastructure.

If the SBCEO discovers or is notified that a breach in the security of SBCEO 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. (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)

If the SBCEO 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. (Education Code 35266)

Safe at Home Program

SBCEO 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 SBCEO 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 County Superintendent of Schools or designee to enact this policy. Instead, they are provided as additional resources for those interested in the subject matter of the policy.

State	Description
5 CCR 16020-16022	Records; general provisions
5 CCR 16023-16027	District records; retention and destruction
5 CCR 430-438	Individual student records
Civ. Code 1798.29	District records; breach of security
Code of Civil Procedure 1985.8	Electronic Discovery Act
Code of Civil Procedure 2031.010-2031.060	Civil Discovery Act; scope of discovery demand
Code of Civil Procedure 2031.210-2031.320	Civil Discovery Act; response to inspection demand
Ed. Code 35145	Public meetings
Ed. Code 35163	Official actions, minutes and journal
Ed. Code 35252-35255	Records and reports
Ed. Code 35266	Cybersecurity
Ed. Code 44031	Personnel file contents and inspection
Ed. Code 49065	Reasonable charge for transcripts
Ed. Code 49069.7	Absolute right to access
Gov. Code 11549.3	Office of Information Security
Gov. Code 12946	Fair Employment and Housing Act: discrimination prohibited
Gov. Code 6205-6210	Confidentiality of addresses for victims of domestic violence, sexual assault, stalking, human trafficking, child abduction, and elder or dependent adult abuse
Gov. Code 6215-6216	Address confidentiality; reproductive health care providers, employees, volunteers, patients, and other individuals who face threats or violence
Gov. Code 7920.000-7930.215	California Public Records Act

Gov. Code 8586.5

Pen. Code 11170

Federal

20 USC 1232g

34 CFR 99.1-99.8

Management Resources

California Secretary of State Publication
State Ed. Tech. Directors Assoc. Pub.

Website

Website

Website

Website

Website

Website

Office of Emergency Services; California Cybersecurity Information Center

[Retention of child abuse reports](#)

Description

[Family Educational Rights and Privacy Act \(FERPA\) of 1974](#)

[Family Educational Rights and Privacy Act](#)

Description

[Records Management Handbook](#)

[Small Districts, Big Hurdles: Cybersecurity Support for Small, Rural, and Under-resourced School Districts, October 2023](#)

[Safe at Home; Schools](#)

[Federal Communications Commission, Schools and Libraries Cybersecurity Pilot Program](#)

[Cybersecurity and Infrastructure Security Agency, Government Coordinating Councils](#)

[California Office of Emergency Services](#)

[CSBA District and County Office of Education Legal Services](#)

[California Secretary of State](#)

ADOPTED BY COUNTY BOARD:

November 13, 2025

REVISED: