Policy 3580: District Records

Status: ADOPTED

Original Adopted Date: 11/01/2009 **| Last Revised Date:** 03/01/2025 **| Last Reviewed Date:** 03/01/2025

CSBA NOTE: The following optional policy and accompanying administrative regulation address the classification and retention of district records pursuant to 5 CCR 16020-16027 and may be revised to reflect district practice. For more information about personnel records, including the contents and retention of such records pursuant to 5 CCR 16023, see AR 4112.6/4212.6/4312.6 - Personnel Files. For additional requirements pertaining to student records, including the contents and retention of such records pursuant to Education Code 49069.7, 5 CCR 430-438, and the Family Educational Rights and Privacy Act (20 USC 1232g and 34 CFR 99.1-99.8), see BP/AR 5125 - Student Records. For requirements pertaining to public access to certain records in accordance with the California Public Records Act (CPRA) (Government Code 7920.000 - 7930.215), see BP/AR 1340 - Access to District Records and BB 9012 - Board Member Electronic Communications.

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.

CSBA NOTE: 5 CCR 16020 defines a "record" as any document which the district is required by law to prepare or retain or which the district prepares or retains as necessary to the discharge of official duty. 5 CCR 16022 requires the Superintendent or designee to annually review and classify these records in order to determine the length of time for which they must be retained. Depending on their content, electronic communications such as email, voicemail, and text messages may also be considered "records" and thus are subject to the same classification and retention schedule as paper documents.

Code of Civil Procedure 1985.8 (the California Electronic Discovery Act) and Code of Civil Procedure 2031.010 describe the procedural rules requiring the disclosure of documents to the opposing party in litigation applicable to electronically stored information. These state statutes are similar to federal Rules of Civil Procedure that apply to actions in federal courts and which also include provisions related to electronically stored information. In general, the rules require parties in litigation to identify and disclose potentially relevant electronic information and, upon notification by district legal counsel of pending or anticipated litigation, halt the routine destruction of paper or electronic records (e.g., suspend automatic monthly erasure of back-up tapes) that could be potentially relevant (a "litigation hold").

It is important that districts have an efficient and consistent system in place for discarding those documents, including email, that are not considered "records." Such a system may help reduce storage costs and prevent unnecessary disclosure. For example, Government Code 7927.500 exempts from disclosure "preliminary drafts" not retained by the district. The purpose of this exemption is to allow a measure of confidentiality for pending district action. However, if preliminary drafts are not regularly discarded, then they may be considered a "record" that has been retained by the district and thus subject to disclosure under the CPRA.

The following optional paragraph, which may be revised to reflect district practice, directs the Superintendent or designee to create a document management system which includes a process for the storage and destruction of electronic materials. Each district will need to do an analysis of the type of system needed based on the size of the district, number of school sites, number of employees, and the type, practice, and capability of the district's information technology system. It is recommended that districts with questions about records retention requirements consult CSBA's District and County Office of Education Legal Services or district legal counsel.

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.

CSBA NOTE: Pursuant to Government Code 8586.5, the California Cybersecurity Integration Center (CSIC) serves as the central organizing hub of the state government's cybersecurity preparedness and response activities. Government Code 8586.5 requires CSIC to coordinate cyber intelligence and information sharing with specified public and private entities, and, as amended by AB 1023 (Ch. 555, Statutes of 2023), requires such sharing of information, including cyber threat information, with school districts. Government Code 11549.3 authorizes districts, at district expense, to request the Military Department, in consultation with CSIC, to perform an independent security assessment of the district or individual district school. Districts are encouraged to consult with

the California Office of Emergency Services and utilize resources such as the State Threat Assessment System and Regional Fusion Centers to help assess potential threats.

Additionally, in an effort to enhance cybersecurity across K-12 schools, the U.S. Department of Education and the Cybersecurity and Infrastructure Security Agency launched the Government Coordinating Council for the Education Facilities Subsector in 2024. Districts who meet the federal universal service discounts for Internet access (E-rate discounts) eligibility requirements may be eligible for funding to purchase cybersecurity services and equipment through the Federal Communications Commission's Schools and Libraries Cybersecurity Pilot Program. The State Educational Technology Directors Association's 2023 guidance, "Small Districts, Big Hurdles: Cybersecurity Support for Small, Rural, and Under-resourced Districts," provides additional information regarding the use of leadership development, partnership building, vulnerability assessment, and staff training to enhance cybersecurity readiness.

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 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.

CSBA NOTE: Pursuant to Civil Code 1798.29, districts are required to disclose any breach of security of any records that contain personal information, as defined. The required formatting and contents of the notification are detailed in Civil Code 1798.29. A district may maintain its own notification procedure as part of an information security policy provided that the notification is consistent with the requirements in Civil Code 1798.29 regarding timing of the notification.

Additionally, pursuant to Education Code 35266, districts that experience a cyberattack, as defined, which impacts more than 500 students or personnel, are required to report such cyberattack to CSIC.

If the district discovers or is notified that a breach in the 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. (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 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. (Education Code 35266)

Safe at Home Program

CSBA NOTE: The Safe at Home address confidentiality program has been in existence pursuant to Government Code 6205-6210 and 6215-6216 to protect victims of domestic violence, sexual assault, stalking, human trafficking, and elder or dependent adult abuse, and members of their households, as well as district employees who face threats of violence, or violence or harassment from the public because of the employee's work for the district. This type of protection has been extended to district employees and Governing Board members who face threats of violence, or violence or harassment from the public because of the employee's work for the district, and, pursuant to Government Code 6205-6210, as amended by AB 243 (Ch. 642, Statutes of 2023), to victims of child abduction and members of their households. Government Code 6207 provides that, when creating a public record, the district may not include actual residences of students, parents/guardians, or employees when a substitute address is designated through the 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)

CSBA NOTE: According to the Secretary of State, a participant's confidential, actual address may only be used to establish student enrollment eligibility and for school emergency purposes. Pursuant to Government Code 6207, a participant's confidential, actual address is not a public record and should not be made available to anyone under any circumstances. For more information regarding establishing district residency when a student or parent/guardian is participating in the Safe at Home/Confidential Address Program, see AR 5111.1 - District Residency.

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.