Attachment 11: Use CSBA Policy As is

CSBA Sample

Board Policy

District Records

BP 3580
Business and Noninstructional Operations

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 modified 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, 5 CCR 430-433, 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 (Government Code 6251-6270), see BP/AR 1340 - Access to 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)

Note: 5 CCR 16020 defines a "record" as any paper or document which the district is required to maintain or which the district prepares or maintains 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.

***Note: Code of Civil Procedure 1985.8 (the California Electronic Discovery Act) and 2031.010 make the procedural rules requiring the disclosure of documents to the opposing party in litigation applicable to electronically stored information. These state rules 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").***

Note: 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 6254 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 Public Records Act.

Note: 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.

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)

***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.***

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)

Comment [J1]: New language to comply with law

(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

Note: The Secretary of State's Safe at Home program creates a confidential address and mail-forwarding program for victims of domestic violence, stalking, or sexual assault. Government Code 6207 provides that, when creating a public record, the district must not include actual residences of students, parents/guardians, or employees when a substitute address is designated through the Safe at Home program. Districts are required to accept the program participation card issued by the Secretary of State and to substitute a post office box as the participant's address.

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)

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. See also AR 5111.1 - District Residency.

Attachment 11: Use CSBA Policy As is

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

Attachment 11: Use CSBA Policy As is

(11/09 4/13) 5/16