SACRAMENTO CITY UNIFIED SCHOOL DISTRICT
BOARD OF EDUCATION

Agenda Item# 11.1

Meeting Date: September 16, 2021

Subject: **Public Hearing: Second Reading of Revised Board Policy 3580 (District Records)**

- ☐ Information Item Only
- ☐ Approval on Consent Agenda
- ☐ Conference (for discussion only)
- ☐ Conference/First Reading (Action Anticipated: _____)
- ☐ Conference/Action
- ☒ Action
- ☐ Public Hearing

Division: Legal Services and Technology Services

Recommendation: Approve revisions to Board Policy 3580

Background/Rationale: State and federal law require that the District develop a secure document management system that provides for the storage, retrieval, archiving, and destruction of District documents. Such documents include electronically stored information (e.g., emails).

In order to ensure the confidentiality of records and safeguard data against damage, revisions are necessary. No prior updates to BP 3580 have occurred since 2001. Such updates include language in the CSBA Gamut model policy.

The District plans to adopt AR 3580, which includes language in the CSBA Gamut model regulation.

Documents Attached:
1. BP 3580 (Redlines)

Estimated Time of Presentation: 10 Minutes
Submitted by: Raoul Bozio, In House Counsel and Bob Lyons, Chief Information Officer
Approved by: Jorge A. Aguilar, Superintendent

Board of Education Executive Summary

Legal Department and Technology Services

Revision to Board Policy (BP) 3580: District Records

September 16, 2021

I. Overview/History of Department or Program

State and federal law require that the District develop a secure document management system that provides for the storage, retrieval, archiving, and destruction of District documents. Such documents include electronically stored information (e.g., emails).

The current version of Board Policy 3580 was adopted in 1998 and revised in 2001. The proposed revisions to Board Policy 3580 are based on the updates provided by the California School Boards Association (CSBA).

The revised board policy includes provisions regarding the District's document management system and processes for notifications concerning breach of security of District records to ensure its records are developed, maintained, and disposed of in accordance with law. AR 3582 furthermore addresses details of timelines for retaining records and processes regarding electronically stored information.

II. Driving Governance:

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level.

California's Education Code sections 35250-35258 pertain to records and reports and the District's requirements regarding the same. *See e.g.,* Cal. Ed. Code § 3254 ("The governing board of any school district may make photographic, microfilm, or electronic copies of any records of the district. The original of any records of which a photographic, microfilm, or electronic copy has been made may be destroyed when provision is made for permanently maintaining the photographic, microfilm or electronic copies in the files of the district, except that no original record that is basic to any required audit shall be destroyed prior to the second July 1st succeeding the completion of the audit.").

Pursuant to California Civil Code section 1798.29(a):

> Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California (1) whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person, or, (2) whose encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security

credential was, or is reasonably believed to have been, acquired by an unauthorized person and the agency that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or usable. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

III. Budget:

The proposed policy is intended to address the District's document management system, including instances of a breach of security of District records. There is no direct budget impact from the revision to this policy.

IV. Goals, Objectives and Measures:

Pursuant to the District's LCAP Goals, this Board Policy meets "Operational Excellence." The goal is to ensure that District records are developed, maintained, and disposed of in accordance with law.

V. Major Initiatives:

This District records policy is critical to ensure the processes for a secure document management system and set forth how staff and others should store, retrieve, archive, and destroy documents. This Board Policy is also critical to maintain the confidentiality of records and establish regulations to safeguard data.

VI. Results:

Approval of revision to Board Policy 3580. Ensure compliance with state and federal law.

VII. Lessons Learned/Next Steps:

Adoption of revised Board Policy 3580 concerning District records. Information and correspondences concerning this matter have previously been shared with the District. Further updates will be provided as necessary.

Sacramento City USD

Board Policy

District Records

BP 3580
Business and Noninstructional Operations

~~District~~

The Governing Board recognizes the importance of securing and retaining district documents. The Superintendent or designee shall ensure that district records ~~shall be~~are developed, maintained, and disposed of in accordance with law ~~and California Department of Education regulations~~, 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)
~~The Superintendent or designee shall establish regulations that define records which are permanent, optional, and disposable and specify how each type of record is to be maintained or destroyed. Any microfilm copies of original records shall be permanently retained.~~

(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 ~~loss~~theft.

~~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 for victims of domestic violence. (Government Code 6207)~~

~~(cf. 1340 - Access to District Records)~~
~~(cf. 3440 - Inventories)~~
~~(cf. 4040 - Employee Use of Technology)~~
~~(cf. 4112.6/4212.6/4312.6 - Personnel Records)~~
~~(cf. 5111.1 - District Residency)~~
~~(cf. 5125 - Student Records)~~
(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)

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:
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-~~6211~~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 ~~pupil~~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:
~~SECRETARY OF STATE~~
~~Letter re: California Confidential Address Program Implementation (SB 489), August 27, 1999~~
WEB SITES
California Secretary of State: http://www.~~ss~~sos.ca.gov/safeathome

Policy SACRAMENTO CITY UNIFIED SCHOOL DISTRICT
adopted: November 16, 1998 Sacramento, California
revised: November 5, 2001
revised: