AP 3722 District Data Security Standards for End Users

Reference:

Family Educational Rights and Privacy Act Regulations, 34 CFR Section 99.3;
Education Code Sections 76200 et seq.;
California Assembly Bill No. 1130 Personal information: Data breaches;
Title 5 Section 59020 et seq.

1.0 This procedure applies to all District students, faculty, and staff and to others granted use of District information and data assets (electronic and paper). An information asset is a definable piece of information that is created, collected, stored, manipulated, transmitted or otherwise used in the pursuit of the District's mission, regardless of the ownership, location, or format of the information. Specific protection requirements are mandated for certain types of data, such as credit card information (PCI), personally identifiable information (PII), or financial data. Consistent use of this procedure will help to ensure that we maintain robust data protection for all District information assets.

2.0 Personally Identifiable Information

2.1 Personally Identifiable Information (PII) is information that either alone or combined could directly identify an individual or make the individual's identity easily traceable. PII includes information that is unique to an individual (Direct Identifier) or can be combined with other information to identify a specific individual (Indirect Identifier). For purposes of this procedure, PII means an individual's first name or first initial and last name in combination with any one Direct Identifier or any combination of Direct/Indirect Identifiers that permits a person's identity to be reasonably inferred by someone who does not have personal knowledge of the relevant circumstances.

2.1.1 <u>Direct Identifiers</u>: Information that relates specifically to an individual, such as: name, social security number, student or employee id, driver's license number, address, telephone number, username or e-mail address, account number, credit card number, and biometric record (e.g., fingerprints).

2.1.2 <u>Indirect Identifiers</u>: Information that is not unique to an individual but that can be combined with other information to identify specific individuals, such as date of birth, place of birth, mother's maiden name, gender, race/ethnicity, geographic indicator, verification data (pet's name, etc.), and passwords.

3.0 Information Classification Guidelines

3.1 The District identifies three classification levels based on information's value, legal requirements, sensitivity, and availability to the public. Aggregate information is classified based upon the most secure classification level. That is, when information of mixed classifications exists in the same file, document, or other written form, then the entire file, document, etc. shall be classified at the most secure classification level. For example, a document with both Level 1 – Confidential and Level 2 – General information would be classified as Level 1-Confidential.

AP 3722 District Data Security Standards for End Users

3.1.1 Level 1 – Confidential: Information used by District operations that may contain SSN's, PII, financial, health, or other sensitive data such as passwords that may harm or damage the District or users if exposed to the public or to unauthorized subjects. Confidential data is intended solely for use within the District and limited to those with a "business need-to-know". These data must be secured and protected at all times and only authorized personnel may access such data. Examples of Level 1 – Confidential Information include:

3.1.1.1 Social Security Number;

3.1.1.2 Driver's license or California identification card number;

3.1.1.3 Account number, credit, or debit card number, in combination with the required security code or password;

3.1.1.4 Medical information (medical history, conditions, etc.);

3.1.1.5 Biometric information (e.g., fingerprints);

3.1.1.6 Private key (digital certificate);

3.1.1.7 Personal health insurance information (e.g., individual policy number, claims, etc.);

3.1.1.8 Personal financial information (e.g., tax exemptions, deductions, etc.);

3.1.1.9 Protected health information;

3.1.1.10 Law enforcement records (e.g., criminal background check results);

3.1.1.11 Legal information (e.g., investigations, attorney/client communication, etc.);

3.1.2.12 Contract information (e.g., sealed bids).

3.1.2 Level 2 – General: Other information not specifically protected, but may result in financial loss, legal action, damage to the District's reputation, or violate an individual's privacy rights if released. General information is vital to District operations and not intended for public knowledge or consumption. General classification includes information only for internal use within the District that must be protected due to proprietary, ethical, or privacy considerations. Examples of Level 2 – General Information include:

3.1.2.1 Banner ID;

3.1.2.2 Student information (e.g., address, gender, date of birth, etc.);

AP 3722 District Data Security Standards for End Users

3.1.2.3 Employee information (e.g., home address, personal telephone numbers, race/ethnicity, employment history, etc.);

3.1.2.4 Alumni information (same as student and employee information);

3.1.2.5 Job applicant information (same as employee information);

3.1.2.6 Donor/patron information (same as employee information);

3.1.2.7 NOCCCD Research (intellectual property);

3.1.2.8 Student directory information – release must comply with AP 5040 and FERPA regulations (student's name, major field of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, degrees and awards received, the most recent previous public or private school attended by the student);

3.1.2.9 Student educational records – release must comply with AP 5040 and FERPA regulations (grades, GPA, test scores, etc.).

3.1.3 Level 3 – Public: Information prepared and approved for the public knowledge and consumption, which is either explicitly defined as public information or intended to be available to individuals both on and off campus. Examples of Level 3 – Public Information include:

3.1.3.1 Employee information (title; work email address, location, and telephone number; position classification; gross salary);

3.1.3.2 Marketing materials;

3.1.3.3 Materials created for public release.

4.0 Standards for Data Ownership

4.1 All District employees are considered data stewards and are responsible for properly handling District data within information systems.

4.2 Managers are responsible for ensuring the information collected in their areas is being stored, used, shared, and retained in accordance with this procedure.

5.0 Standards for Data Collection

5.1 Information collection should only be made where such collections are essential to meet the authorized business purpose and mission of the District. Examples of information collection include web forms, surveys, account creation, payment transactions, etc.

AP 3722 District Data Security Standards for End Users

5.2 All District employees should regularly review their data collection procedures and purpose to determine whether it is still relevant and necessary for the District's business. Regular review should take place each semester at a minimum.

6.0 **Standards for Data Storage**

6.1 All District employees should use a District-managed secure storage system as their primary data storage location.

6.2 Data from the Level 1 – Confidential category should always be stored in a District-managed secure storage system. Level 1 – Confidential information should never be stored outside of the District-managed secure storage system, such as on a personal hard drive, removable media (USB Drive), personal cloud storage, etc.

6.3 Data from the Level 2 – General categories may only be stored on removable media (e.g., USB Drive, personal cloud storage, external hard drive, etc.) for specific business purposes and need to be encrypted.

7.0 **Standards for Data Use and Transmission**

7.1 All District employees should perform day-to-day work using the minimum appropriate level of information. For example, if work only requires Level 2 – General information, do not include Level 1 – Confidential information in the task.

7.2 All District employees should use a secure connection to access institutional information systems (e.g., Banner, Argos).

7.3 All District employees should use an NOCCCD-managed secure storage system to transmit and share Level 1 – Confidential and Level 2 – General data with other authorized users. Level 1 – Confidential and Level 2 – General information may also be shared using other electronic transmission (e.g., email) so long as the file is encrypted and/or anonymized (PII removed from the file).

8.0 **Standards for Data Retention**

8.1 All District employees should regularly review their holdings of previously collected Level 1 – Confidential and Level 2 – General information to determine whether it is still relevant and necessary for the District's business purpose. Regular review should take place at a minimum of once per semester.

8.2 All District employees should delete and/or anonymize (remove PII from the file for long-term storage) any electronic records no longer necessary for the District's business purpose.

8.3 Federal, state, or other programs, including various student aid or grant programs, may require longer retention periods and such program requirements shall take precedence over the requirements contained herein. Managers are responsible for ensuring the information in their area is retained according to the most appropriate requirements.

AP 3722 District Data Security Standards for End Users

9.0 **Standards for Data Sharing and Data Agreements**

9.1 Third parties who will access unitary Level 1 – Confidential or Level 2 – General District information to perform a service will sign the NOCCCD Confidentiality and Nondisclosure Agreement and return to the Vice Chancellor of Educational Services and Technology before gaining access to such information.

9.2 Third parties interested in requesting unitary District data for research and educational program improvement purposes should enter into a data-sharing agreement specifying the data need, data purpose, data scope, method of secure information transfer (e.g., secure ftp server), and plan for reliable and secure data storage and destruction. Data sharing agreements shall be approved by the Vice Chancellor of Educational Services and Technology before any data are shared. Alternatively, third parties could request to participate in the local research review process for project-specific requests at one of the District institutions or the District site for approval.

9.3 All shared information shall remain the property of the District and shall not be disclosed to any outside institution or individual not specifically mentioned in the NOCCCD Confidentiality and Nondisclosure Agreement and/or Data-Sharing Agreement.

Date of Adoption: May 23, 2022 District Consultation Council