Data Governance Manual

SEPTEMBER 2022

Santa Clara County Office of Education

TABLE OF CONTENTS

TABLE OF CONTENTS

CHAPTER 1.
DATA GOVERNANCE MANUAL

The **Santa Clara County Office of Education (SCCOE)** believes that the value of data as an institutional resource is increased through its widespread and appropriate use. The SCCOE strives to achieve the overall management of the integrity, availability, and security of data used in the organization through the design and implementation of a Data Governance Program.

The Santa Clara County Office of Education promotes an approach both rooted in ethics and equity in managing data as a part of its life cycle. Ethics are a set of moral principles concerned with rights, responsibilities, use of language, what is and is not acceptable, and how decisions are made. Equity is removing the predictability of success or failure that currently correlates with any social or cultural factors. All employees are encouraged to approach data with an equity- centered lens and mindset to ensure data is collected, analyzed, interpreted, and shared with diverse partners without bias or exclusion. The fundamental purpose of using data for equity is to improve understanding of the outcomes a system is producing. Data is used to help ask the questions about the system that will help the organization to make changes to the system.

Data governance is the SCCOE's formal and comprehensive set of policies and processes designed to ensure the ethical management of data throughout its entire life cycle. Data governance establishes responsibility for data, and enables staff to collaboratively and continuously make legal and ethical decisions about the organization's information assets. Through the systematic creation and enforcement of policies, roles, responsibilities, and processes, data governance encourages robust data privacy, security and quality. The Data Governance Program provides a common vision for data use that is aligned with the goals of the SCCOE with the creation of policies and processes in five program areas: Data Privacy, Data Security, Data Architecture and Integration, Data Quality, and Data Literacy.

This manual outlines guidance in each of the program areas; links to relevant documentation and resources are included. The first iteration of the manual focuses on basic guidance for SCCOE employees in Data Privacy and Data Security for student education data and systems; general information and guidance in the other program areas is presented as it is currently available. The manual will be periodically reviewed and updated to include new policies and processes as they emerge as well as to evaluate existing processes after they have been implemented. All SCCOE employees are encouraged to reach out to the Data Governance Coordinator and/or program area leads with any input, questions, and/or comments.

CHAPTER 2.
DATA GOVERNANCE OPERATIONS

MANUAL DEVELOPMENT AND MAINTENANCE

This manual is a living document and will be updated with time as new policies and processes are developed for SCCOE employees in the five Data Governance Program Areas. Additionally, existing policies and processes will be periodically reviewed and adjusted as necessary.

Development of policies and processes shall be led by the Data Governance Coordinator and the Data Governance Committee; Data Stewards and Data Consumers shall offer input as necessary to assist in the drafting of the policies with final approval by the Executive Committee. After approval, the Data Governance Coordinator and the Data Governance Committee shall work with Data Stewards and Consumers to implement the new policies and processes and document them within this manual. Each version and date updated of this document shall be indicated on the bottom of the document (footer); major changes/ updates in each version shall be documented at the beginning of the manual and highlighted. Any edits or changes (approved by the Data Governance Committee or the Executive Committee as applicable) will only be made by the Data Governance Coordinator to ensure version control.

DOCUMENTATION

Not all documentation, especially detailed instructions for role-specific functions, needs to be captured in the data governance manual; staff will be directed to keep/maintain their own documentation and provide access to data governance groups if requested.

PROJECT MANAGEMENT & TIMELINES

The Data Governance Coordinator and the Data Governance Committee shall develop annual work plans to develop any policy or processes within Data Governance Program areas with input from the Executive Committee, Data Stewards, and Data Consumers.

Various annual tasks are assigned to groups or individuals within the Data Governance Charter and Manual; updates (completion and outstanding items) are expected upon request. Leads of program areas and working groups are expected to monitor the progress of assigned tasks and report issues/problems with meeting timelines to the Data Governance Coordinator.

CHAPTER 3.
FRAMEWORKS & PROCESSES

Data Governance Program Area 1.
DATA PRIVACY & CONFIDENTIALITY

Lead: Irina Shacter

Introduction

The SCCOE's SP 0441 Data Governance Policy outlines mandatory compliance with data privacy laws; this section of the DG Manual provides employees guidance to ensure this compliance in the areas of student education data collection, access, use, and sharing. Current guidance focuses on student education data but employees are expected to follow any and all applicable data privacy laws for other types of data.

The SCCOE promotes an approach both rooted in ethics and equity in managing data as a part of its life cycle. Ethics are a set of moral principles concerned with rights, responsibilities, use of language, what is and is not acceptable, and how decisions are made. Equity is removing the predictability of success or failure that currently correlates with any social or cultural factors. All employees are encouraged to approach data with an equity- centered lens and mindset to ensure data is collected, analyzed, interpreted, and shared with diverse partners without bias or exclusion. The fundamental purpose of using data for equity is to improve understanding of the outcomes a system is producing. Data is used to help ask the questions about the system that will help the organization to make changes to the system.

A basic tenant of Ethics and Equity in Data Privacy is doing no harm to the people represented in the data. With laws and policies as the legal floor in decision-making regarding data privacy, decisions around using and sharing data should include ethical/equity considerations which cultivate public trust.

Section 1.1. Student Data Laws & Regulations

SCCOE is dedicated to protecting the privacy and rights of individuals in accordance with federal, state, and local laws and treats all student personally identifiable information (PII) as private and confidential information. Certain student data are required based on legal obligations, to protect the vital interests of students, for public interest, and legitimate educational interests of staff and third parties but shall not be exposed to unauthorized individuals, agencies or external sources unless legally permissible. Students, families/guardians, and districts should expect that personally identifiable data maintained or stored by SCCOE staff and systems is safe, properly cared for, and used only for appropriate purposes. This applies to SCCOE employees, interns, volunteers, and consultants, and third-parties who receive or have access to SCCOE's data and/or data systems and encompasses all systems, automated and manual, including systems managed or hosted by third parties on behalf of SCCOE and it addresses all information, regardless of the form or format, which is created or used in support of the activities of SCCOE.

SCCOE staff are expected to understand and follow applicable laws and regulations around the collection, use, disclosure, and destruction of student data. Employees that are observed not following legal requirements on student data privacy will be subject to disciplinary action; an effort will be made to meet with the employee and provide necessary training as needed. Continued disregard to following legal requirements will result in disciplinary action as determined by the employee's direct supervisor.

CHAPTER 3.
FRAMEWORKS & PROCESSES

The Family Educational Rights and Privacy Act (FERPA) is a federal law that guarantees parents access to their children's educational record and restricts who can access and use these records. Local education agencies (LEAs) may share PII educational records without parental consent under certain circumstances (e.g., another school system regarding a student's enrollment/transfer, financial aid, accrediting organizations, to comply with a judicial order or subpoena, health/safety emergencies, and local and state authorities, within a juvenile justice system) or exceptions (listed below). LEAs must notify parents of their rights under FERPA annually and ensure notices on directory information, surveys, and data collection.

- Directory Information is student PII that is generally not considered harmful or an invasion of privacy if released and can also be disclosed to outside organizations without a parent/guardian's prior written consent. Each LEA must determine the list of fields it classifies as "Directory Information" and give parents the opportunity to opt out of their student's information being shared; per Education Code section 49073, directory information may not be released regarding a pupil identified as a homeless child/youth. FERPA does not require recordation of the release of directory information.

  The SCCOE defines "directory information" as: name, address, telephone, date of birth, email address, major field of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, diplomas and awards received, and most recent previous educational institution attended.

- School Officials are persons that have a legitimate educational interest in accessing student PII. Each LEA must define "school official" and "legitimate educational interest". FERPA does not require recordation of the release of PII to school officials with legitimate educational interest.

  The SCCOE defines a school official as "persons employed by the District as an administrator, supervisor, instructor, or support staff member (including health or medical staff and District-employed law enforcement personnel), a Board member, a person or company with whom the District has contracted to perform a special service (such as an attorney, auditor, medical consultant, or therapist), or a parent, student, foster family agency, short-term residential treatment staff, or caregiver whose access to student records is legally authorized. A "legitimate educational interest" is one held by a school official or employee whose duties and responsibilities create a reasonable need for access. (Ed. Code, §§ 49063(d), 49076, 49076.5; 20 U.S.C. § 1232g)"

- Studies are the disclosure of PII from student education records must be for, or on behalf of, an educational agency or institution, in order to develop, validate, or administer predictive tests; administer student aid programs; or improve instruction.

  Audit/Evaluation is the disclosure of PII from education records must be to audit or evaluate a Federal- or State-supported education program; or enforce or comply with Federal legal requirements related to the program.

The Individuals with Disabilities Education Act (IDEA) is a law that makes available a free appropriate public education to eligible children with disabilities throughout the nation and ensures special education and related services to those children. IDEA includes privacy provisions that are similar but more strict than FERPA to protect the privacy of PII.

CHAPTER 3.
FRAMEWORKS & PROCESSES

The National School Lunch Program (NSLP) provides low-cost or free school lunch meals to qualified students through subsidies to schools. NSLP safeguards the confidentiality of students receiving free and reduced-price school meals as it has stricter privacy provisions than FERPA in who may have access to records on students who are eligible for free and reduced-price meals.

The Protection of Pupil Rights Amendment (PPRA) applies to the programs and activities of a state education agency (SEA), local education agency (LEA), or other recipient of funds under any program funded by the U.S. Department of Education. It governs the administration to students of a survey, analysis, or evaluation that concerns one or more of the following eight protected areas. In order to administer such surveys, schools must be able to show parents any of the survey materials used, and provide parents with choices (opt out) for any surveys that deal with certain sensitive categories.

- political affiliations or beliefs of the student or the student's parent;
- mental or psychological problems of the student or the student's family;
- sex behavior or attitudes;
- illegal, anti-social, self-incriminating, or demeaning behavior;
- critical appraisals of other individuals with whom respondents have close family relationships;
- legally recognized privileged or analogous relationships, such as those of lawyers, physicians, and ministers;
- religious practices, affiliations, or beliefs of the student or student's parent; or
- income (other than that required by law to determine eligibility for participation in a program or for receiving financial assistance under such program).

The Health Insurance Portability and Accountability Act (HIPAA) is a national standard that protects sensitive patient health information from being disclosed without the patient's consent or knowledge. Via the Privacy Rule, the main goal is to ensure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well-being; the law requires security of health information in electronic form and applies only to covered entities (health plans, health care providers, and health care clearinghouses). HIPPA provisions rarely apply in the educational setting as student educational records, even most medical information collected and maintained by schools, are subject only to FERPA.

The Children's Online Privacy Protection Act (COPPA) controls the information collected from children under 13 by companies that operate websites, games, and mobile applications. Teachers are authorized to provide consent for parents if the program or application is used for educational purposes.

The Student Online Personal Information Protection Act (SOPIPA), which came into effect in 2015, is a California state law which prevents online companies from compiling K-12 student data for marketing or advertising purposes. The law is unique in that it puts responsibility for protecting student data directly on industry by expressly prohibiting education technology service providers from selling student data, using that information to advertise to students or their families, or "amassing a profile" on students to be used for noneducational purposes. In addition, the law requires online service providers to ensure that any data they collect is secure and to delete student information at the request of a school or district.

CHAPTER 3.
FRAMEWORKS & PROCESSES

The California Constitution provides rights to privacy; every effort should be made to protect the privacy of students' information even if the information is not expressly protected by the laws listed above.

Section 1.2. Data Classification

Data elements carry varying levels of risk and sensitivity based on the risk for harm from an unauthorized or inadvertent disclosure. The SCCOE shall maintain a list of data elements that are classified by their sensitivity; to see the current Data Classification chart, please see Appendix A. SCCOE Data Stewards are charged with creating documentation of data elements within their respective data systems, especially the systems that hold elements high in sensitivity.

Section 1.3. Data Collection

Student data collected and stored in systems built or maintained by the SCCOE shall follow FERPA and any other pertinent laws and regulations in collecting data only that is necessary to collect.

SCCOE Data Stewards shall create and maintain a catalog of data elements collected/stored within their respective systems. Data Stewards and other partners, as applicable, shall review data elements collected and determine if any need to be added or deleted with the approval of the Data Governance Committee, Executive Committee, and/or partners, as applicable. To see the current Student Data System Inventory, please see Appendix B.

Section 1.4. Data Access – Data Systems

The SCCOE will ensure any systems it develops or maintains with such data to serve the needs of LEAs or other public agencies will have appropriate levels of security to ensure data available can only be viewed or accessed by parties legally allowed to do so. Only staff and third parties (e.g., vendors) with legitimate educational interest shall be granted access to any system holding student data; users should be placed in appropriate user roles that limit access to data elements that are critical to their job responsibilities. Student data system users are expressly prohibited from sharing their login information with others or any PII data from the system with other individuals (e.g., exporting data and sharing with others and/or logging into a data system during a meeting/training with individuals that do not have access to said system). Employees should not export any PII data out of a data system unless expressly authorized to do for a job function; employees must follow guidance provided in this document in *Section 2.6 (Data Security Guidance)* and *Section 1.7 (Data Reports and Presentations)*, as applicable.

SCCOE Data Stewards shall develop/maintain documentation on the processes employees gain access, security roles and the data elements that are accessed by each role, as well as perform an annual audit of users. Data Consumers that have access to data systems or elements they should not have access to need to notify the corresponding SCCOE Data Steward immediately (see Appendix B for SCCOE Student Data Systems Inventory).

Section 1.4. Data Access – Data Files

All recipients must maintain the confidentiality of the data to which they have access and understand that the information included in any files are to be restricted to only those authorized to access the information. SCCOE staff should always document student data they share in a written data sharing agreement. Data shall always be shared in a secure manner, shall not be forwarded to any additional parties, and shall be destroyed when the use is complete (see *Section 2.6. Security Guidance* for more information).

CHAPTER 3.
FRAMEWORKS & PROCESSES

Section 1.5. Data Use

Student data shall only be used for purposes granted under FERPA, other applicable laws, an/or any other agreements between the SCCOE and other partners.

Section 1.6. Data Sharing Agreements

SCCOE staff must comply with all state and federal laws and regulations on student data collection, use, storage, and sharing; no student data shall be shared by SCCOE employees without a written agreement. At minimum, the agreement must outline: the recipient of the data/systems access, the data elements shared/given access to as well as the level of access (e.g., PII, de-identified, aggregated), the reason for sharing (why is the data needed and will be done with the data), as well as time/duration for the agreement. Memorandums of Understanding (MOUs) and Contracts that involve student data shared by SCCOE employees must adhere to the provisions outlined in SP 3294 Partnerships and Memorandums of Understanding in regards to review of said MOU or contract by the Data Governance Department. The Data Governance Department will provide guidance and technical assistance to SCCOE employees to ensure that the proper provisions for data privacy and security are included; additional data sharing agreements and/or permission forms may be needed.

SCCOE student program staff who wish to purchase an application from a vendor should review the California Student Privacy Alliance vendor database for a previously signed agreement between a vendor and an educational institution; staff will then be able to join an existing agreement with the vendor by using Exhibit E. If a vendor is not listed, staff is encouraged to ask the vendor to sign a CA-NPA especially when student PII is stored/accessed by the vendor. Vendors who do not agree to sign the agreement will be approved on a case by case basis by TDSD and DG staff. Vendors not agreeing to sign the CA-NPA and other entities wishing to have access to SCCOE student educational records PII should have offer a data sharing agreement that has the following provisions outlined: a purpose/reason for sharing, the list of data elements, restrictions (collection, use, storage, and sharing) outlined in applicable laws, and terms for data destruction. SCCOE TSDS and Data Governance staff will review the data privacy and data security information and advise program staff on next steps.

The SCCOE does not require a data sharing agreement for staff receiving student data from external partners for the purposes of their roles/responsibilities. SCCOE staff receiving/accessing student PII are required to follow student data privacy laws, keep the data secure (see *Section 2.6 Data Security Guidance – Files*), and uphold the stipulations of any data sharing agreements they sign.

Section 1.7. Data Reports and Presentations

SCCOE staff making public reports derived from students' education records must perform an analysis of the data and apply statistical disclosure limitation methods to remove any PII from those reports prior to release. Unless expressly permitted by law, no student PII data shall be shared in data reports or presentations with internal or external collaborators. Employees must ensure that data is deidentified or redacted.

Suppression rules are to be followed in accordance to protecting student privacy. SCCOE staff should follow California Department of Education guidelines of suppressing any counts below 11 students to prevent the identification of students based on combining indirect identifiers; this is especially important in data sets that contain various demographic variables in which the identity of the student may be compromised. The

CHAPTER 3.
FRAMEWORKS & PROCESSES

FERPA standard for de-identification assesses whether a "reasonable person in the school community who does not have personal knowledge of the relevant circumstances" could identify individual students based on reasonably available information, including other public information released by an agency, such as a report presenting detailed data in tables with small size cells. The "reasonable person" standard should be used by state and local educational agencies and institutions to determine whether statistical information or records have been sufficiently redacted prior to release such that a "reasonable person" (i.e., a hypothetical, rational, prudent, average individual) in the school community should not be able to identify a student because of some well-publicized event, communications, or other similar factor. School officials, including teachers, administrators, coaches, and volunteers, are not considered in making the reasonable person determination since they are presumed to have inside knowledge of the relevant circumstances and of the identity of the students. Refer to the Future of Privacy Forum's Guide to Practical De-identification as needed.

Section 1.8. Data Breaches

The SCCOE diligently works to ensure that data breaches do not occur, either from a *systems breach* (cyber attack) or *user error* (inadvertent disclosure of PII data to unauthorized persons) through the implementation of policies, processes, and training.

Section 1.8.1 Data Breach Incident Response

In the event of an unauthorized release, disclosure or acquisition of student data that compromises the security, confidentiality or integrity of the student data maintained by the SCCOE, SCCOE shall follow the protocol outlined in SCCOE's Data Breach Incident Response Plan. The plan is owned and implemented by the Technology & Data Services Division.

Section 1.8.2 Data Breach Reporting

A user error breach has happened if an SCCOE employee receives files containing sensitive information or PII, and said employee was not the intended recipient. Employees that receive data that was not intended to be sent to them should always alert the sender; not open the files and delete the email/files immediately. Trash folders should be immediately emptied when they contain sensitive emails and files.

If an SCCOE employee sends files containing sensitive information or PII to unintended recipients, they need to immediately contact the recipient and ask them to permanently delete the files and report the incident via ServiceNow.

Section 1.9. Training

As part of the Data Governance program, designated employees shall participate in mandated annual training on such topics as data privacy and data security.

CHAPTER 3.
FRAMEWORKS & PROCESSES

Data Governance Program Area 2.
DATA SECURITY

Lead: Vince Tran

Introduction

The SCCOE's SP 0441 Data Governance Policy outlines mandatory compliance with data privacy laws; this section of the DG Manual outline the organization's commitment to securely handling data by protecting data within the technology infrastructure and providing guidance for staff on the proper and appropriate use of SCCOE's applications and tools.

The SCCOE promotes an approach both rooted in ethics and equity in managing data as a part of its life cycle. Ethics are a set of moral principles concerned with rights, responsibilities, use of language, what is and is not acceptable, and how decisions are made. Equity is removing the predictability of success or failure that currently correlates with any social or cultural factors. All employees are encouraged to approach data with an equity- centered lens and mindset to ensure data is collected, analyzed, interpreted, and shared with diverse partners without bias or exclusion. The fundamental purpose of using data for equity is to improve understanding of the outcomes a system is producing. Data is used to help ask the questions about the system that will help the organization to make changes to the system.

Ethics and Equity in Data Security rests on the unwavering belief that everyone's data deserves to be protected throughout its lifecycle. In the area of Data Security, there is a commitment to best practices which involve the adoption of tools and procedures to ensure secure handling of data. All data is valuable and must be protected ethically and equitably.

Section 2.1. SCCOE Employee Use of Technology

All SCCOE employees are required to adhere to all guidance around data security including, but not limited to: use of data, use of security tools for data transfer, and password guidance.

For more information, please refer to the newly updated AR 4040 Employee Use of Technology (ETA October 2022).

Section 2.2. Cybersecurity Framework

The adoption and ongoing implementation/auditing of a cybersecurity framework is a key component of keeping data secure. The SCCOE has adopted the CIS cybersecurity framework and will work to continuously audit and update practices as needed.

Section 2.3. Data Breaches

The SCCOE diligently works to ensure that data breaches do not occur, either from *systems breac*h (cyber attack) or *user error* (inadvertent disclosure of PII data to unauthorized persons) through the implementation of policies, processes, and training.

CHAPTER 3.
FRAMEWORKS & PROCESSES

Section 2.3.1. Data Breach Incident Response

In the event of an unauthorized release, disclosure or acquisition of student data that compromises the security, confidentiality or integrity of the student data maintained by the SCCOE, SCCOE shall follow the proper protocol outlined in SCCOE's Data Breach Incident Response Plan. The plan is owned and implemented by the Technology & Data Services Division.

Section 2.3.2. Data Breach Reporting

If an employee suspects that a systems breach has occured, they need to immediately report the incident via ServiceNow.

Section 2.4. Asset Management

Asset management is the process of receiving, tagging, documenting, and eventually disposing of equipment. It is critically important to maintain up to date inventory and asset controls to ensure computer equipment locations and dispositions are well known. Lost or stolen equipment often contains sensitive data. Proper asset management procedures and protocols provide documentation that aid in recovery, replacement, criminal, and insurance activities.

If an employee's device that contains PII or other sensitive data is lost or stolen, the employee shall notify their supervisor and log a ticket in via ServiceNow.

Section 2.5. Data System Inventory

The organization shall maintain a complete up-to-date inventory of all data systems (e.g., those that store and process data) as it enables staff to target its data security and privacy management efforts to appropriately protect PII and sensitive data.

Section 2.6. Data Security Guidance- Files

All SCCOE employees must adhere to the processes outlined below when sending/receiving, collecting, and storing personally identifiable information (PII) and non-publicly available data going forward. The following instructions are for files/data sets that live outside of a database or program used to house student data (e.g., DataZone, Aeries, etc) and apply to student data and where applicable, all institutional data.

Section 2.6.1. SCCOE Security Tools

There are a number of tools available to you to properly handle sensitive email and data. The SCCOE is committed to providing staff the necessary training to be able to know how to use these tools and when to use them depending on the situation. Any department or individual needing training or instructions on use of any tool below, or for support/issues and for enhancements, submit a ticket via ServiceNow.

Encrypting your **email** will ensure that your message will only be able to be read by your intended recipients. Email encryption is available on all SCCOE email accounts. Staff are responsible for knowing how and when to encrypt emails to recipients outside of the SCCOE; for step-by-step instructions, view the ServiceNow Knowledge Base – Email Encryption. Internal COE-to-COE staff emails do not risk being intercepted because it all stays in the Microsoft internal cloud. Therefore, email encryption is not the proper security tool to be used when sending internal emails that contain PII or non-publicly available information.

CHAPTER 3.
FRAMEWORKS & PROCESSES

The SCCOE email system will automatically encrypt any messages sent by SCCOE staff which contain potential PII detected within the message or attachments. Email messages received from outside SCCOE which contain potential PII will be rejected, with both the sender and recipient notified to take appropriate actions to protect the message before resending.

LaserFiche is document management software used by many SCCOE staff. Because it is a system hosted by SCCOE, users can be confident that data put into LaserFiche is fully secure. Besides being a document repository, the LaserFiche system can also be used to gather data with surveys or other form-based methods. Data collected with the LaserFiche system is subject to strict security protections and policies. Staff may reach out to TDSD for more information on LaserFiche and to determine if it is the correct application to be used for handling, collecting and storing data.

Microsoft OneDrive is the modern replacement for user home folders. This is an online, personal folder in which users should store their files. An advantage of using Microsoft OneDrive is the ease with which users can share files with others within and outside the organization. Files shared directly from OneDrive can also easily be unshared, thereby giving users an easy method to securely manage their own files. For more information on how to use OneDrive to share files, please visit the ServiceNow Knowledge Base.

CHAPTER 3.
FRAMEWORKS & PROCESSES

To securely receive or provide multiple files to outside parties, including vendors, customers and partner organizations, **SecureShare** is a platform that is both easy and secure to use. Outside parties will have a web interface where they can easily drop files for SCCOE staff retrieval. Similarly SCCOE staff may deposit files into the application, where others can securely retrieve the files. The interface allows the SCCOE user to set file expiration dates, or access details which further allows secure management of sensitive files. This is a licensed product, and programs will have to acquire licenses through the SCCOE technology department. For more information on how secure a license and use the SecureShare platform, please visit the ServiceNow Knowledge Base.

The **Google** ecosystem cannot be used to collect, store or transfer student PII. While Google offers an array of very effective collaboration tools, the Google environment is not a safe platform for PII. Many functions which are critical for handling PII, such as recoverability, auditability, reporting, and enforcing correct access privileges to sensitive data are not available or inadequate in Google. For these reasons, the SCCOE strongly recommends handling PII information and data files via the other approved platforms described in this document.

Section 2.6.2. Other Considerations

Due to the changing requirements and demands for remote work, staff are needing to shift their practices and adapt to new ways of handling data. Staff should always use SCCOE-issued devices when working from home and handling PII. By using SCCOE devices, users can be confident that the data stored on, received and sent from them the device is fully protected. SCCOE hard drives are encrypted to ensure that in the event the device is lost or stolen, that PII cannot be retrieved off of the device. All SCCOE computers have virtual private networks (VPN) automatically enabled. Staff may confidently connect to remote wireless connections, whether at home or elsewhere outside of the office, with the knowledge that data sent to and received from SCCOE systems are protected. If a SCCOE device is lost or stolen, and staff are aware that it contains PII, they must notify your supervisor and technology support immediately.

It is common practice to add SCCOE email and other SCCOE-approved applications to personal devices. This is also called bring-your-own-device (BYOD). Personal devices can be added to SCCOE networks and used to access email and other applications such as Microsoft Teams. Sending and receiving PII is not to be done on personal devices. Important security functions such as encryption are limited on mobile phones. When sending and receiving PII and other data and attachments that require encryption and special handling, use only your SCCOE-provided device, such as a laptop or desktop. PII files in attachments, which should always be protected, may be downloaded and stored in an approved location (see above). If you receive emails with PII attachments or other content, reading the email is safe. However responding to the message, or downloading the attachment should be done on the SCCOE-provided device. This guidance also applies to other SCCOE applications that are installed on personal devices such as Microsoft Teams.

Section 2.6.3. Receiving Data Files

SCCOE staff should always demonstrate good practices around data privacy and security (see SCCOE SP 4040). When expecting a file from an external partner (district, parent, etc.), SCCOE employees should have an established and agreed upon method in place with the other party for receiving confidential or sensitive

information. When districts or other organizations do not have secure channels for data sharing, SCCOE staff should initiate a secure communication channel that the sender can respond to with the data file(s); examples are detailed below:

- An encrypted email (available to all SCCOE staff)
- SecureShare (if SCCOE employee has a license)
- OneDrive (for when real-time collaboration is necessary)
- SFTP (for large files, volume, frequency; e.g., DataZone)

Employees that receive data that was not intended to be sent to them should always alert the sender; not open the files and delete the email/files immediately. Trash folders should be immediately emptied when they contain sensitive emails and files.

Section 2.6.4. Sending Data Files

It is important to carefully consider if PII information being sent is necessary to send/share. If an employee does need to send/share PII, they should use one of the following approved methods of sharing.

Acceptable ways to send files include encrypted email with PII in an attachment, OneDrive, and SecureShare. Staff should be aware that email encryption does not work when sending emails internally, that is, from one SCCOE staff member to another.

Additionally, staff should include the following reminder to receivers of data files:

ATTENTION: This [mode of communication] contains personally identifiable or confidential information for the sole use of the intended recipient. All recipients must maintain the confidentiality of the data to which they have access and understand that any review, copying, or distribution of this data to others is strictly prohibited. Data should always be shared and stored in a secure manner and should be destroyed when the use is complete. If you are not the intended recipient of this data, please contact the sender immediately and permanently delete the original and any copies of this [mode of communication].

Section 2.6.5. Collecting Data

SCCOE staff may find it necessary to collect/generate student PII data.

Only approved systems, outside of existing systems that store student data (Appendix B) may be used to collect sensitive PII data. Currently the only systems which may be used to collect PII in a survey or for general PII data gathering is the SCCOE LaserFiche system or through Microsoft OneDrive (see Appendix C). Laserfiche is capable of creating survey applications, collecting the data, maintaining strict access control to the data, and presenting reports and other outputs for data usage. Additionally, employees may create/store PII in a shared OneDrive folder for projects that require collaboration/ongoing access to the dataset by approved parties.

Other tools such as SurveyMonkey and Google are not appropriate for collecting PII data since they are not secure and are not able to be protected by the SCCOE Technology Department.

CHAPTER 3.
FRAMEWORKS & PROCESSES

Section 2.6.6. Storing Data Files

Employees may need to store files they have received or generated from a data system to perform analyses or other approved functions. The guidance below outlines where to store, and not store, non-publicly available information.

Acceptable storage locations include: H drive/Home folder, OneDrive, and LaserFiche. Do not store non-publicly available information on Google Drive, desktop folders, USBs, external hard drives, or personal devices.

Section 2.7. Data Destruction

One of the last decisions to be made in the data lifecycle comes when specific data are no longer needed for the purposes for which they were originally collected and stored. Data destruction is the process of removing information in a way that renders it unreadable (for paper records) or irretrievable (for digital records).

Data files should be destroyed once they are no longer needed for any authorized purpose. SCCOE staff are responsible for knowing when sensitive files are no longer needed, and then deleting/destroying the file permanently. Trash folders containing sensitive files must be emptied.

Employees that receive data that was not intended to be sent to them should always alert the sender; not open the files and delete the email/files immediately. Trash folders should be immediately emptied when they contain sensitive emails and files.

CHAPTER 3.
FRAMEWORKS & PROCESSES

Data Governance Program Area 3.
ARCHITECTURE & INTEGRATION

Lead: Narasimhan Ganesh

Introduction

This program area outlines guidance to standardize the collection, storage, transformation, distribution and use of data to allow for the integration of disparate data systems and data sets to make data accessible to authorized users.

The SCCOE promotes an approach both rooted in ethics and equity in managing data as a part of its life cycle. Ethics are a set of moral principles concerned with rights, responsibilities, use of language, what is and is not acceptable, and how decisions are made. Equity is removing the predictability of success or failure that currently correlates with any social or cultural factors. All employees are encouraged to approach data with an equity- centered lens and mindset to ensure data is collected, analyzed, interpreted, and shared with diverse partners without bias or exclusion. The fundamental purpose of using data for equity is to improve understanding of the outcomes a system is producing. Data is used to help ask the questions about the system that will help the organization to make changes to the system.

Data Integration is becoming a powerful tool in ethically and equitably informing policy decisions, supporting research on effectiveness of programs, and bringing together holistic/wraparound supports for students and systems. Ethics and equity in Data Integration aids in the coordination of services and can reduce the burden on individuals when procuring services. It is the responsibly of data collectors and consumers to distinguish when data should be integrated and to ensure that the integration of data sets does not contribute to misleading interpretations of data.

Section 3.1. Master Data Management

SCCOE TDSD staff and/or Data Stewards shall create and maintain technical infrastructure to support master data management. Each Data Steward shall identify the single source of record and make the single source of record accessible to all intended users.

Section 3.2. Data Matching

SCCOE Data Stewards shall identify, implement, and maintain algorithms for automated matching, as applicable. Each Data Steward will 1) establish, implement, and maintain resolution processes for near matches using manual reviews and 2) establish, implement, and maintain processes to standardize data, decouple shared IDs, merge duplicates, and eliminate incomplete or erroneous records.

Section 3.3. Access Controls

SCCOE Data Stewards shall ensure that any new system, data set from a known/existing data source, or data set from a new entity/agency included in the existing technical architecture has appropriate access controls. Access controls include controls regarding who can access a system (systems access) as well as what data elements users can access within the system as appropriate for their job responsibilities (role-based access).

CHAPTER 3.
FRAMEWORKS & PROCESSES

Section 3.4. Adding New Participating Organizations and/or Data Sets

The addition or change to any data system built or maintained by the SCCOE is classified as a critical data issue. When considering an addition or a change to any data system that holds student data, SCCOE program staff should include various teams in the conversations around integration, privacy and security well in advance of implementation by submitting a request for evaluation by contacting Rodrick Ang, Product Manager.

The following sections include some, but not all, of the key considerations SCCOE program staff shall consider in submitting for evaluation and due diligence for adding new participating organizations and/or data sets.

Section 3.4.1 Introduction of New System

When introducing a new system that holds student data, the project team and/or the SCCOE will need to clearly identify the following:

- Complete scope of the new system and all included data elements
- Highlight the data security and privacy controls that are in place
- Mitigations for any gaps with security and privacy controls
- For a vendor hosted solution, it should highlight
  - where the service is hosted, and
  - who has access to services and systems associated with it.
- If the new system replaces an existing system, the organization need to make sure data is purged from the old system. If the old system was a vendor hosted system, the vendor must provide a written confirmation of safe removal of data from their system.

Section 3.4.2 Data Integration Requirements

Prior to integrating any data between two systems, SCCOE Data Stewards need to evaluate if the source or the destination system have any student PII data. Stewards also need to determine the system or organizational ownership of the data to ensure integrity of the source of truth is not altered during the integration process. Integration of two systems needs to be done in a safe and secure manner. If the integration is based on files exchanged between two systems, exchange should happen through a secure file transfer system with limited and administrative access to personnels. Where possible, files should be encrypted for additional data protection. If it is an API based data exchange, it should not be an open API and should be authenticated via secure credentials or tokens. Data flow between two systems should be reviewed by the data steward including adherence to well established data standards.

Section 3.4.3 Access Controls

SCCOE Data Stewards need to evaluate the access requirement for the new system based on the sensitivity of the information in the system. Systems should be able to support single sign-on and where possible integrated with a two-factor authentication system. Systems should also include role-based access controls to allow need based access to data.

CHAPTER 3.
FRAMEWORKS & PROCESSES

Data Governance Program Area 4.
DATA QUALITY

Lead: Dharma Jayabal

Introduction

Guidance in this program area ensure that employees follow data management best practices, thus ensuring data is accurate, timely, consistent, and meets partner needs.

The SCCOE promotes an approach both rooted in ethics and equity in managing data as a part of its life cycle. Ethics are a set of moral principles concerned with rights, responsibilities, use of language, what is and is not acceptable, and how decisions are made. Equity is removing the predictability of success or failure that currently correlates with any social or cultural factors. All employees are encouraged to approach data with an equity- centered lens and mindset to ensure
data is collected, analyzed, interpreted, and shared with diverse partners without bias or exclusion. The fundamental purpose of using data for equity is to improve understanding of the outcomes a system is producing. Data is used to help ask the questions about the system that will help the organization to make changes to the system.

Ethics and equity in Data Quality is the responsibility of all employees given that they play an important role in data entry and collection. Proper policies and procedures related to the handling of data is critical to ensure that data consumers have insights to any errors, bias, etc. prior to using the data to make decisions.

Section 4.1. Data Standards

All SCCOE staff shall take steps to assure that student data they collect or process into any data system is complete and accurate in the first instance; following SCCOE or vendor guidance of how and where the data should be entered. Data must be accurate and updated in such a way as to give a true picture of the current situation of the student. Data Stewards must have available vendor guidance on standards or guidance developed for internally built and maintained systems.

Section 4.2. Data Inventory

The organization shall create and maintain a complete up-to-date inventory of all data that are collected as well as all data systems—including those used to store and process data— as it enables the agency to target its data security and privacy management efforts to appropriately protect PII and sensitive data. To see the SCCOE's current Student Data Systems Inventory, see Appendix B.

CHAPTER 3.
FRAMEWORKS & PROCESSES

Section 4.3. Critical Data Issues

The SCCOE defines a critical data issue as a problem with data that has an impact on data quality and use. Examples can include:

- Changes to laws/regulations that impact data definitions, calculations, access rights
- Changes (deletion or addition) to data sets or systems
- Changes to vendor-hosted products
- Data errors
- Lack of accessibility to data systems (systems being down)

Section 4.3.1. Changes to Data Sets, Systems, Products

Changes to data sets, systems, and/or vendor products ar defined as critical data issues; please see *Section 3.4. Adding New Participating Organizations and/or Data Sets.*

Section 4.3.2. Data Errors

The SCCOE shall correct data which it knows to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the legal guardian does not request rectification. Inaccurate data must be erased and replaced by corrected or supplemented data.

Data consumers must report any data quality (e.g., missing or incorrect data) issues they encounter within a data system to the appropriate Data Steward (see Appendix B). Data Stewards must correct any data quality issues, as applicable. If escalation is required, data stewards shall contact the Data Governance Coordinator and the Data Governance Program Area- Data Quality lead to determine the path to resolution. If applicable, the Data Governance Coordinator shall convene a meeting of the Data Governance Committee and/or Executive Committee to determine the path to resolution.

Section 4.4. Data Quality Audits

SCCOE Data Stewards will, as applicable, create and document processes for preventing, detecting, and preventing data errors in the systems that they oversee.

Section 4.5. Data Requests

Section 4.5.1. Publicly Available Data

To ensure SCCOE employees are using and sharing publicly available datasets in a consistent manner, employees should only use trusted sources and cite their sources within presentations, reports, etc. It is the responsibility of SCCOE staff to ensure that they are providing accurate data and should ensure that any data products provided to internal or external partners are reviewed by another staff member.

Section 4.5.2. SCCOE Data Requests

SCCOE employees needing help locating or accessing student data (e.g., publicly available data, CALPADS, or SCCOE's DataZone Student Data Warehouse) or creating a data product can submit an Internal Data Request via ServiceNow; additional permissions may be required prior to receiving the requested dataset or report.

CHAPTER 3.
FRAMEWORKS & PROCESSES

Data Governance Program Area 5.
DATA LITERACY

Lead: Karen Larson

Introduction

This guidance outlines the skill set required to ensure data consumers can turn data into useful information.

The SCCOE promotes an approach both rooted in ethics and equity in managing data as a part of its life cycle. Ethics are a set of moral principles concerned with rights, responsibilities, use of language, what is and is not acceptable, and how decisions are made. Equity is removing the predictability of success or failure that currently correlates with any social or cultural factors. All employees are encouraged to approach data with an equity- centered lens and mindset to ensure data is collected, analyzed, interpreted, and shared with diverse partners without bias or exclusion. The fundamental purpose of using data for equity is to improve understanding of the outcomes a system is producing. Data is used to help ask the questions about the system that will help the organization to make changes to the system.

Data Literacy is the ability to read, write and communicate data in context. This includes understanding data sources, analytical methods, and the ability to describe the use case, application, and value of the data. Data literacy is also the ability to use existing and emerging technologies in service of managing and making meaning from data sets. Therefore, ethics and equity in Data Literacy means that there are ways in which data producers and data consumers are provided with the necessary learning opportunities to develop their data skills. Training is available to all employees who handle data and takes into account their experience and role in the lifecycle of the data.

CHAPTER 3.
FRAMEWORKS & PROCESSES

Section 5.1. Data Literacy Overview

Data Literacy is the ability to transform information into actionable knowledge and practices by collecting, analyzing, and interpreting all types of data (assessment, school climate, behavioral, snapshot, longitudinal, moment-to-moment, etc.) to help determine next steps. For educators, data literacy combines an understanding of data with standards, disciplinary knowledge and practices, curricular knowledge, pedagogical content knowledge, and an understanding of how children learn. (Gummer and Mandinach)

Not only are hard skills necessary to be effective with data, but the dispositions and habits of mind are critical to the successful implementation and integration of data into the user's everyday life. Without these softer skills, data literacy as a skill set and a process for informing decisions and change will be ineffective. These habits of mind or factors that influence data use include:

- Belief in data,
- Belief in continuous iterative cycles for improvement,
- Ethical use of data,
- Collaboration,
- Communication,
- Belief in using data to pursue equity.

The Santa Clara County Office of Education promotes an ethical and equity-centered approach to data literacy. Data equity applies an equity-centered lens and mindset to ensure data is collected, analyzed, interpreted, and shared with diverse partners without bias or exclusion. It enables data consumers to make informed decisions by ensuring all partners are authentically engaged throughout the data cycle. To create positive changes in outcomes, leaders should model data literate behaviors, as well as provide the conditions and resources for inquiry teams to examine data deeply by looking beyond the disaggregation of quantitative data sets to identify achievement gaps and examine data that is often qualitative and typically not part of our state and federal report submissions.

Data literate individuals:

- know the different kinds of data that exist and which kind of data to use for which decision
- evaluate the accuracy and sufficiency of each kind of data they will use
- transform data from a variety of sources (classroom, school, district, state) into actionable information to guide decisions
- hold themselves accountable for ethical generation, interpretation, and application of assessment data

Ethical and responsible data literacy is knowing how to use data, and that knowledge focuses on how to protect student privacy and maintain confidentiality of student information. Such knowledge includes how, when, and with whom to discuss students' performance, behavior, attitudes, etc. Addressing student data privacy is included in the Data Literacy Framework.

Data informed decision making in all aspects of education, therefore data literacy is a critical skill for educators and those who support educators.

CHAPTER 3.
FRAMEWORKS & PROCESSES

Section 5.2. Data Literacy Framework

Working in a data literate environment requires an infrastructure that supports key components of data literacy and depositions and habits of mind in order to effectively integrate data seamlessly and equitably into the daily cadence of work. As outlined in this manual, the infrastructure includes a robust organizational and technology structure, as well as an informed user base. Users, including educators and those who support educators, work collaboratively within a cycle of continuous improvement using a framework that further educates and supports the use of data to continuously improve student learning.

Section 5.2.1. Identify Problems & Frame Questions

When beginning an inquiry cycle, it is important for educators and those supporting educators to be able to articulate a problem of practice about a student, group of students, a topical area, the curriculum, or an aspect of instruction. Educators should be able to identify the problem and explain the issue or question. Additionally they should be able to know the context at the student level. By contextualizing the learning, behavioral, or motivation issues students experience, educators will better understand the situation, will more accurately identify the problem, make a decision to address the problem, and follow through on subsequent action.

Understanding the context at the school level is also important. This is a different level of aggregation from student level context. Understanding the larger context of a school in which teachers' practice is embedded provides a broad view toward seeking solutions to problems of practice.

Additional participants or partners, including students, should be involved in this process. Other educators, parents, and students can provide valuable insights into students' performance. Consultation with them is an important part of the decision-making process.

Understanding student privacy is critical. It is increasingly important for all participants to understand the regulations around the protection of student privacy and confidentiality. This skill set includes, among other topics, knowing how to discuss data and with whom, and understanding data sharing.

Section 5.2.2. Use Data

This component is a composition of diverse skills and knowledge that generally fall under the category of using data.

Understanding data sources entails understanding the differences between qualitative and quantitative data, knowing how to identify the right data sources for the problem, understanding data quality and data properties, understanding the purposes of different data sources, understanding the alignment of different data sources to the problem of practice, and knowing how to use multiple sources of data.

Another set of skills deals with the access of data: knowing how to locate and retrieve data sources and familiarity with technologies to support data use. For example, knowing how to access DataZone, the CDE Dashboard, the SCCOE Data Service Tracker, and other relevant resources.

CHAPTER 3. FRAMEWORKS & PROCESSES

A third set of skills focuses on a general understanding of fundamental concepts of statistics and psychometrics (with no intention of creating measurement specialists or statisticians). Psychometrics is a field of study within psychology concerned with the theory and technique of measurement. Psychometrics generally refers to specialized fields within psychology and education devoted to testing, measurement, assessment, and related activities. Educators need a fundamental knowledge of psychometrics, including topics such as reliability, validity, and error of measurement.

A fourth subcomponent focuses on how to handle data. This entails knowing how to generate, analyze, prioritize, integrate, examine, manipulate, organize, manage, aggregate, and disaggregate data. It also entails knowing how to drill down into data and knowing the appropriate level of data that pertains to the problem of practice. When analyzing, manipulating, aggregating, and disaggregating data, it is important that data consumers keep data equity and ethics front of mind.

A final set focuses on the use of assessments. This entails knowing how to develop assessments, select assessments for particular purposes, and knowing the differences across various types of assessments.

Section 5.2.3. Transform Data Into Information

Skills here include fundamental statistics, understanding data displays and representations, how to assess patterns and trends, the summarization and synthesis of data, understanding of and predicting the consequences of decisions, and understanding how to interpret data. When transforming data into information, it is important that data consumers consider how that information may be used in equitable or inequitable ways.

Section 5.2.4. Transform Data Into Decisions

This component focuses on the translation of the data and information into instructional action or some other kind of action. Educators should have the ability to determine what to do instructionally, based on the information they have, and the ability to diagnose the problem and make appropriate instructional adjustments. It also focuses on the differentiation of data use for individual students and groups of students, versus whole class instruction.

Section 5.2.5. Evaluate Outcomes

The final component deals with examining the outcomes of a decision, comparing the changes that have occurred because of the implementation of some course of action, whether instructional or something else. It requires educators to compare pre and post results, monitor for student and classroom changes, and reconsider the original issue that was posed.

The component is not seen as the end of the inquiry cycle but rather that data-informed decision making is an iterative process. It may require another pass through the inquiry process before a successful outcome has been accomplished. hen evaluating decision outcomes, data consumers should intentionally and thoughtfully consider how implicit bias and cultural differences may be impacting the outcome and if there are ways to put in place controls to mitigate data inequity.

CHAPTER 3.
FRAMEWORKS & PROCESSES

Section 5.3. The Continuous Improvement Cycle

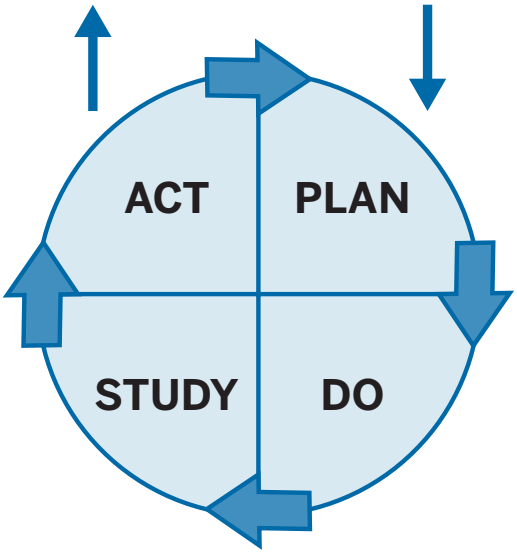
Working within a system that provides a structure and time to review and reflect on its processes in light of its results is important. Using a Plan, Do, Study, Act Cycle, or PDSA, is one way to determine steps to effect change, then reflect on the process. Below is a PDSA model and a link for more information.

The Carnegie Foundation's white paper on continuous improvement in education can be found here.

What specifically are we trying to accomplish?

What change(s) might we introduce and why?

How will we know that a change is actually an improvement?



"The Model for Improvement" @2009 API

Section 5.4. Use Cases

Student Data Privacy and Data Ethics Scenarios is a useful document outlining numerous examples of situations when school personnel may be faced with decisions on how to handle student data. The scenarios begin with a table of contents by topic on page 20 and is divided by topics ranging from the handling of data to classroom practices. Each scenario presents the situation and a user's guide that outlines what we know, questions for further discussion, and unintended consequences.

CHAPTER 4. GLOSSARY

Architecture & Integration: Standardize the collection, storage, transformation, distribution and use of data to allow for the integration of disparate data systems and data sets to make data accessible to authorized users.

Critical data issue: A problem with data that has an impact on data quality and use. Examples can include: changes to laws/regulations that impact data definitions, calculations, access rights, changes (deletion or addition) to data sets or systems, changes to vendor-hosted products, data entry errors, and/or lack of accessibility to data systems (systems being down)

Data: Facts, ideas, or discrete pieces of information, especially when in the form originally collected and unanalyzed.

Data Access: The right/ability to read, enter, copy, query, download, or update data, which is potentially different for different sets of data for each person, role, etc.

Data Consumer: A person or organization who uses data for a specific purpose and can be affected by its quality. A data consumer has authorization to procure data by means of direct access or through any product or system through the SCCOE.

Data Content Management: Identify purposes for which data are collected. Communicate purposes to staff and customers. Review collection policies regularly.

Data Breach: Disclosure of data to unauthorized persons, either as a systems breach (cyber attack) or user error (inadvertent disclosure).

Data Destruction: The process of removing information in a way that renders it unreadable (for paper records) or irretrievable (for digital records).

Data Ethics and Equity: The consideration, through an equity lens, of the ways in which data is collected, analyzed, interpreted, and distributed and that this is done without bias or exclusion. The fundamental purpose of using data for equity is to improve understanding of the outcomes a system is producing. Data is used to help ask the questions about the system that will help the organization to make changes to the system.

Data Governance: A formal and comprehensive set of policies and practices designed to ensure the ethical management of data throughout its entire life cycle within SCCOE—encouraging robust data security, privacy, quality, and integration. It establishes responsibility for data, organizing staff to collaboratively and continuously make legal and ethical decisions about the organization's information assets through the systematic creation and enforcement of policies, roles, responsibilities, and procedures in all data governance program areas.

Data Literacy: The ability to transform information into actionable knowledge and practices by collecting, analyzing, and interpreting all types of data (assessment, school climate, behavioral, snapshot, longitudinal, moment-to-moment, etc.) to help determine next steps.

CHAPTER 4. GLOSSARY

Data Privacy/Confidentiality: Compliance with all relevant federal and state privacy and confidentiality laws and regulations are followed for data collection, data access, data use, and data sharing agreements.

Data Records Management: Develop and adhere to policies that define how records should be created, maintained, and deleted.

Data Security: Technical aspects of protecting the data within the technology infrastructure and user applications and tools.

Data Stewards: Employees that are in positions that 1) review data before it is submitted or released for reporting, 2) own a particular data system (e.g., built or maintain it from a technical perspective), and/or 3) have deep knowledge of the data in the system (update frequency, data flows, definitions, and/or business rules). Technical data stewards oversee the actual systems that allow the system to function (e.g., import, code for the application, server, authentication); business data stewards oversee the non-technical components of the system (e.g., direction of the system, implementation of the system, collaboration within SCCOE and agencies/others (if applicable), and/or promotion).

Data Quality: The planning, implementation, and control of activities that apply quality management techniques to data to ensure it is fit for consumption and meets the needs of data consumers.

Directory Information: Student PII that is generally not considered harmful or an invasion of privacy if released and can also be disclosed to outside organizations without a parent/guardian's prior written consent.

Disclosure: Permits access to or the release, transfer, or other communication of personally identifiable information contained in education records by any means, including oral, written, or electronic means, to any party except the party identified as the party that provided or created the record (FERPA 20 U.S.C. 1232g and 34 CFR Part 100).

Education Records: Records, files, documents, and other materials which contain information directly related to a student; and are maintained by an educational agency or institution (FERPA, 20 U.S.C. § 1232g(a)(4)(A)).

Institutional Data: The data that is gathered, stored, analyzed, and published by the SCCOE in support of its overall mission and goals.

Legitimate Educational Interest: Held by a school official or employee whose duties and responsibilities create a reasonable need for access. (Ed. Code, §§ 49063(d), 49076, 49076.5; 20 U.S.C. § 1232g).

CHAPTER 4. GLOSSARY

Personally Identifiable Information (PII): Information that can be used to distinguish or trace an individual's identity either directly or indirectly through linkages with other information.The term includes, but is not limited to (FERPA 20 U.S.C. 1232g and 34 CFR Part 99)—

(a) The student's name;

(b) The name of the student's parent or other family members;

(c) The address of the student or student's family;

(d) A personal identifier, such as the student's social security number, student number, or biometric record;

(e) Other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name;

(f) Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or

(g) Information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record Relates.

School Officials: Persons that have a legitimate educational interest in accessing student PII. Each LEA must define "school official" and "legitimate educational interest".

APPENDIX A: DATA CLASSIFICATION

Classification	Description	Examples
Prohibited	This data is prohibited from being collected from students.	Social Security Number (SSN), Immigration Status
Highly Sensitive PII	The dataset includes highly sensitive information that is kept confidential at all times and is only accessible by a small group of authorized personnel. Release of misuse of this data would be very damaging to individuals.	Special Education Details (IEP, assessment results), Mental Health Records, Social Security Number, Data outlined in PPRA
Sensitive PII	The dataset includes sensitive information that is kept confidential at all times and is accessible by individuals and groups on a need to know basis. Release of misuse of this data could be damaging to individuals.	Special Ed Details (Disability Type), 504 Details (Disability Type), FRL, SED, Foster Youth, Homeless/McKinney Vento, Migrant Ed
Sensitive PII	The dataset includes sensitive information that is part of a students record that can be accessed by most authorized groups in a system. Release or misuse of this data could result in some harm to associated groups or individuals.	Special Ed Status (Yes/No), 504 Status (Yes/No), Language Proficiency, Suspension data, Expulsion Data, Graduation status, Grades, A-G Completion, Assessment Results
General PII	The dataset includes general information that is part of a students record that can be accessed by most authorized groups in a system. Release or misuse of this data could be concerning to associated groups or individuals.	Course Enrollment, School Enrollment, GPA
General	The dataset includes general information that is part of a student's record that can be accessed by all authorized groups in a system. Release or misuse of this data could be uncomfortable to associated groups or individuals, but likely would not result in harm.	Directory Information, Publicly Available Data, Aggregated Data, De-identified Data

APPENDIX B: SCCOE STUDENT DATA SYSTEMS INVENTORY

Data System	Data System Description	Data Steward – Technical	Data Steward – Business
Aeries – SCCOE Student Programs Only	Student Information System (SIS)	Kevran Day, Database Administrator II	Norma Bayless, Transition Coordinator, Alternative Education; Duong Ton, Student Services Specialist, Special Education
Assessment Application – DataZone	An SCCOE application allows for DataZone districts to create and manage local assessments, record student assessment results, and track student progress across domains.	Dharma Jayabal, Manager, Data Systems	Meaghen Spencer, Manager, Data Services
California Educator Reporting System (CERS)	The California Educator Reporting System (CERS) allows teachers and administrators to access their students' individual and aggregate test results from state summative and interim assessments. To access CERS, educators must use their assigned Test Operations Management System (TOMS) credentials.	California Department of Education	Dan Mason, Manager-Assessment & Accountability
California Longitudinal Pupil Achievement Data System (CALPADS)	A longitudinal data system used to maintain individual-level data including student demographics, course data, discipline, assessments, staff assignments, and other data for state and federal reporting.	California Department of Education	Kevran Day, Database Administrator II
Canvas	Learning Management System (LMS)	Karen Larson, Director III, iSTEAM	Karen Larson, Director III, iSTEAM
Child Care Portal	The Santa Clara County Childcare Portal is managed by the Santa Clara County Childcare Resource & Referral Program and contains regularly updated information about all licensed childcare providers in the county. Families searching for care can find local programs that best meet their needs through the search feature and may request information directly from multiple providers by creating a portal account.	Daniel Jin, Data Systems & Communications Specialist	Veronica Garza, Manager, Early Childhood Integrated Data Systems

APPENDIX B: SCCOE STUDENT DATA SYSTEMS INVENTORY

Data System	Data System Description	Data Steward – Technical	Data Steward – Business
ChildPlus	The student information system (SIS) for the Head Start & Early Head Start Programs.	Harry Tong, HeadStart Program Analyst; Kevran Day, Database Administrator II	Maria Scallia, Supervisor, Administrative Services
ClassDojo	ClassDojo helps to keep parents up to date on student progress and classroom happenings.	SCCOE TDSD	James Howarth, Assitant Director, Special Ed; Jennifer Casel, Manager, Special Ed Programs
Clever	Single Sign On (SSO)	Ilona Sparks, Applications System Analyst	N/A
ContinuumCloud (formerly Welligent)	A cloud-based electronic health record (EHR) system.	Narasimhan Ganesh, Director III, Data & Analytics Development	Chaunise Powell, Executive Director, Youth Health & Wellness
DataZone (DZ)	DataZone is a data warehouse and an analytics platform that provides teachers and leaders with valuable student data.	Dharma Jayabal, Manager, Data Systems	Nabil Shahin, Director III, K12 Data Governance
Desired Results Developmental Profile (DRDP) Online	An evidence-based educational assessment tool. Teachers use the DRDP (2015) to track the development of children enrolled in early care and early childhood educational programs.	Harry Tong, HeadStart Program Analyst	Araceli Foncesca, Manager, EL Program Operations
Document Tracking Services (DTS)	Document Tracking Services (DTS) is an easy-to-use web service that streamlines the process of updating template-based documents, translations, online forms hosting and cloud-based document storage for compliance purposes.	Vendor	Laura Aguilar, Sr. Administrative Assistant; Duong Ton, Student Services Specialist

APPENDIX B: SCCOE STUDENT DATA SYSTEMS INVENTORY

Data System	Data System Description	Data Steward – Technical	Data Steward – Business
FosterVision (FV)	An SCCOE data analytics tool available to monitor foster youth data across disparate systems and allows staff responsible for foster youth the ability to easily access and monitor a student's portfolio. Educational data is sourced from SCCOE's DataZone Student Data Warehouse and combined with agency data which allows for better monitoring and support of foster youth students.	Eric Sandoval, Web Developer/ Programmer, LD	Nabil Shahin, Director III, K12 Data Governance
HandsOn	Captures attendance during the sign In & out icluding meal tracking& reports.	Eric Sandoval, Web Developer/ Programmer, LD	John Gomez, Manager, Program & Quality Assurance
Imagine Learning (formerly Edgenuity)	Online Learning Platform	Ilona Sparks, Applications System Analyst	Eugene Santillian, Principal, Alternative Education; James Howarth, Assistant Director, Special Education
LaserFiche	Content management platform	Jim Carrillo, Director III, Applications, Business & Web Systems	Varies based on project owner
Learning Genie	An app utilized by teachers to log DRDP data.	Harry Tong, HeadStart Program Analyst	Kristen Lee, Manager, ELS/ Planning & Support; Araceli Foncesca, Manager, EL Program Operations
Medical Billing Technologies (MBT)	Collects information inputted by Medi-Cal billable service providers related to services; sends information for reimbursement.	Medi-Cal Billing	Ruby Nevarez, Student Services Specialist

APPENDIX B: SCCOE STUDENT DATA SYSTEMS INVENTORY

Data System	Data System Description	Data Steward – Technical	Data Steward – Business
Migrant Student Information Exchange (MSIX)	A national web-based portal that links states' migrant student record databases. It facilitates the national exchange of migrant students' educational and health records among the states. MSIX produces a single "consolidated record" from each state in which a migrant child was ever enrolled. MSIX provides information on student's previous moves, enrollments, grade or course placement, and accrual of credits.	U.S Department of Education	U.S Department of Education
Migrant Student Information System (MSIN)	A state-wide system developed and managed by WestEd. Integrated with California's longitudinal student data system, the MSIN serves as a central student information system for the state's migrant student population. WestEd has partnered with CDE for almost two decades to support the Migrant Education Program, and help ensure that every migrant student has access to the appropriate education supports they need to succeed in school.	Karen Balderas, Enrollment Data Specialist; Israel Rivera Alvarado, Enrollment Data Specialist, LD; Simi Pannu, Supervisor, Migrant Ed ID&R	U.S Department of Education
Naviance	Naviance is a web-based, comprehensive college and career readiness platform for high school students that helps students and families connect what students learn in their studies to their life goals. Naviance empowers students to create a plan for their future by helping them discover their individual strengths and learning styles. In the Naviance database, students explore and research colleges and careers based on their personal skills and areas of interest.	Vendor	Vendor
NoHo	The student information systems for the CSPP & CCTR Programs.	John Gomez, Manager, Program & Quality Assurance	Maria Scallia, Supervisor, Administrative Services

APPENDIX B: SCCOE STUDENT DATA SYSTEMS INVENTORY

Data System	Data System Description	Data Steward – Technical	Data Steward – Business
Parentsquare	ParentSquare is a communication application for teachers, administrators, students and parents. ParentSquare allows both administrators and teachers to post messages to parent through private messages or class/school wide messages. Administrators and teachers are also able to post surverys, questionnaires, ask parents to upload documents when needed.	Vendor	Jennifer Casel, Manager, Special Ed Programs; Duong Ton, Student Services Specialist
ReadyRosie	ReadyRosie is an early education tool that helps families, schools, and communities across the nation deepen and scale their family engagement efforts.	Harry Tong, HeadStart Program Analyst	Kristen Lee, Manager, ELS/Planning & Support
Renaissance Star (RenStar)	Local assessment for math and literacy.	Tracy Rhofling, Coordinator, State & Federal Programs Alternative Education; Phil Morales, Director/ Principal, OYA; Katherine Everett, Assistant Principal, OYA	Charlotte Biggerstaff, Student Assessment Technician, Alternative Education; Phil Morales, Director/ Principal, OYA; Katherine Everett, Assistant Principal, OYA
RIM	An SCCOE developed systems that allows districts to upload releveant student information for SCCOE to review for student placement and itinerant services.	Donna Xia, Web Developer/ Programmer, SR	Ruby Nevarez, Student Services Specialist
Schoology	K12 Learning Management System	Vendor	Vendor
Special Education Information System (SEIS)	A web-based system that allows centralized, online access for writing IEPs, managing special education data, CALPADS reporting, and service tracking.	N/A	Kimberly Dang, SELPA Data & Program Administrative Support Specialist (South East SELPA)

APPENDIX B: SCCOE STUDENT DATA SYSTEMS INVENTORY

Data System	Data System Description	Data Steward – Technical	Data Steward – Business
ServiceLink (SLS)	An SCCOE application provided to SLS coordinators via the SCCOE Data Management System and allows School Linked Services coordinators to log referrals to Behavioral Health Services. The app tracks student referrals to services and monitors if the students were successfully "linked" to service(s). The referrals are then stored in the application's database and matched with data elements from the SCCOE's DataZone Student Data Warehouse.	Eric Sandoval, Web Developer/ Programmer, LD	Meaghen Spencer, Manager, Data Services
SIRAS	A comprehensive web based program that provides online management of IEP, 504 and SSTs.	Diana Franco, Education Program Analyst, Special Education; Catherine Mendoza, Program Specialist, OYA	Catherine Mendoza, Program Specialist, OYA
Test Operations Management System (TOMS)	Test Administrator Interface for All Online Tests.	California Department of Education	Dan Mason, Manager, Assessment & Accountability
Ultracamp	Online registration system for outdoor school and summer day camp.	Tad Nakamura, Environmental Ed Program LD; Ron Lauder, Environmental Ed Program LD; Moriah Wright, Health Technician, Environmental Ed	Marie Bacher, Director II, Environmental Ed

Data stewards are employees that are in positions that 1) review data before it is submitted or released for reporting, 2) own a particular data system, or 3) have deep knowledge of the data in that system. Technical Data Stewards oversee the actual systems that allow the system to function while Business Data Stewards oversee the non-technical components of the system.

APPENDIX C: APPROVED DATA COLLECTION SYSTEMS

Type of data being collected	What is the risk associated with this data being insecurely stored?	What is the appropriate system to collect/store this data?
Sensitive data (8 topics covered by PPRA*) tied to a student *explicit parent consent is required before collecting this information from students	High	LaserFiche, OneDrive
Data that is tied to a student (SSID, Name) that is not sensitive (not covered by PPRA)	Low/Moderate	LaserFiche, OneDrive
Data that is not tied to a student (de-identified)	Low	SurveyMonkey, Google Forms, etc

Santa Clara County Office of Education

1290 Ridder Park Drive, San Jose, CA 95131

www.sccoe.org