Cal-PASSPlus

Partnership for Achieving Student Success

www.calpassplus.org

California Partnership for Achieving Student Success

Privacy and Security Policies and Procedures

Version 3.0

Updated January 2019

Description of Cal-PASS Plus

Mission:

Cal-PASS Plus is an initiative that collects, analyzes and shares student data in order to track performance and improve success from preschool through college and into the workforce. Cal-PASS Plus represents a new approach to improving education. Through the Cal-PASS Plus project, leaders involved in the education to workforce pipeline can learn the answers to questions such as:

- How do my students do when they leave my institution?
- Were they well prepared? Are adjustments in curriculum or program necessary to improve their preparation?
- How many got degrees? What did they get degrees in? How long did it take?

Cal-PASS Plus is a simple and very practical approach that helps educators and stakeholders:

- Understand student performance, including transition
- Improve instruction
- Increase student success

Partners:

California school districts (Pre-K through high school), community colleges, colleges and universities are participating in this partnership.

Authorization, funding and privacy:

Cal-PASS Plus operates with funding from the State of California under a grant from the California Community Colleges Chancellor's Office as well as several grants by local foundations. The Cal-PASS Plus website is operated on behalf of the California Community Colleges Chancellor's Office (CCCCO). Cal-PASS Plus and the CCCCO are committed to protecting your privacy and the personal information collected via this website. This privacy policy applies solely to the Cal-PASS Plus website and does not apply to any other websites that you may be able to access from this website, each of which may have data collection, storage and use practices and policies that differ materially from this privacy policy. By using this website, you agree to this privacy policy, and consent to the data practices described herein.

1.0 Privacy: Cal-PASS Plus and FERPA

The protection and privacy of student academic records is governed by the Family Educational Right to Privacy Act (FERPA) at the federal level and under the California Code of Regulations at the state level.

Appendix A of this document contains the complete text of FERPA. Below is an excerpt from The Family Educational Right to Privacy Act (Buckley Amendment) that covers Cal-PASS Plus activities.

> *(F) organizations conducting studies for, or on behalf of, educational agencies or institutions for the purpose of developing, validating, or administering predictive tests, administering student aid programs, and improving instruction (emphasis added), if such studies are conducted in such a manner as will not permit the personal identification of students and their parents by persons other than representatives of such organizations and such information will be destroyed when no longer needed for the purpose for which it is conducted;*

Cal-PASS Plus exceeds the privacy requirements of FERPA because personally identifiable student record information is not being disclosed in the data sharing process; however, assuming that personally identifiable student information was being transferred, such transfer is allowed by FERPA in 20 U.S.C. Section 1232g(b)(1)(F). That subsection reads in relevant part that education records may be released to "*organizations conducting studies for, or on behalf of educational agencies or institutions for the purpose of . . . improving instruction, if such studies are conducted in such a manner as will not permit the personal identification of students and their parents by persons other than representatives of such organizations and such information will be destroyed when no longer needed for the purpose for which it is conducted*."

The sole purpose of Cal-PASS Plus is to carry out the transfer and exchange of student academic data for the purpose of improving instruction. Student academic data is sent to Cal-PASS Plus, which shares it with institutions that are identified via the governing MOU and data-sharing agreement. MOU-holding partners use the data to study student achievement as it relates to a variety of variables, such as level of courses taken within a given discipline; academic grades achieved; test scores; and other data which is used to evaluate the effectiveness of the institution's instructional programs. Analysis of Cal-PASS Plus data is also used by the sharing institutions to assist in identifying bright spots and scaling best practices, to inform placement practices and to align educational programs with labor market demand. Notwithstanding the foregoing, the actual process used by Cal-PASS Plus is such that no personally identifiable data is retained once the submitted data has been loaded into the data warehouse. This file submission takes place over SSL-encrypted protocol and files are never stored on our web servers (not even temporarily). They

are immediately deposited into the secure storage, not accessible via Internet. It is more secure than FTP (SFTP, or FTPS).

When institutions choose to submit data through our **validator system**, the sending institution encrypts all data before it is sent to the Cal-PASS Plus server. This process is accomplished through Cal-PASS Plus encryption software that is downloaded and run on the institution's computer. The information received by Cal-PASS Plus is identified only by a series of digits and letters in which no name or social security number could be identified. Names and social security numbers do not exist in the data set. Each student's set of data becomes an anonymous set identified by the identification number that is created by the encryption software. Thus, the data is anonymous and personally identifiable information is not being transferred.

When institutions choose to submit data through our **drag and drop loader**, the sending institution submits their files to the Cal-PASS Plus server via a Secure Socket Layer connection. All personally identifiable information is removed by the Cal-PASS Plus loader program and the original submitted files are encrypted and stored only until the load program completes the process of adding the new information to the Cal-PASS Plus data warehouse. No personally identifiable information is retained once the submitted data has been loaded into the data warehouse.

2.0 Data Sharing Agreements

All access to data (in the aggregate or unitary records) is based on the Data Sharing Agreement attached to the participating institution's MOU.

3.0 Electronic Transfer

The Cal-PASS Plus project is committed to ensuring the privacy and maintaining appropriate confidentiality standards for all students and institutions participating in Cal-PASS Plus.

When data are submitted by a Cal-PASS Plus member for inclusion in the main database, certain safeguards and rules apply.

3.1 Submission of data through our validator software

Prior to submission and at the Cal-PASS Plus member site, a Cal-PASS Plus data validation software program replaces all student identifiers with a pseudo ID and creates upload files that appear as simply a string of numbers and letters. No personally identifiable information is transmitted to the Cal-PASS Plus server. All records are transmitted to the repository server via Secure Socket Layer with a user ID that is an alphanumeric, case sensitive, 8-character password. The Cal-PASS Plus

servers employ application level security, Windows level security and database level security for access into the data repository.

3.2 Submission of data through our drag and drop loader

The sending institution submits their files to the Cal-PASS Plus server via a Secure Socket Layer connection. All personally identifiable information is removed by the Cal-PASS Plus loader program and the original submitted files are encrypted and stored only until the loader program completes the process of adding the new information to the Cal-PASS Plus data warehouse. No personally identifiable information is retained once the submitted data has been loaded into the data warehouse. All records are transmitted to the repository server via Secure Socket Layer with a user ID that is an alphanumeric, case sensitive, 8-character password. The Cal-PASS Plus servers employ application level security, Windows level security and database level security for access into the data repository.

3.3 Problems with submissions

Occasionally, a Cal-PASS Plus participant may require assistance from the Cal-PASS Plus Database Administrator to troubleshoot a problem in the creation of the submission file. This often requires the participant to send their working file for identification of the problem. If the participant is unable to utilize the File Upload feature to transmit the file, in order to employ a secure transmission of the file(s), a password protected folder is created on a secure FTP site for the participant to submit the file. The Database Administrator retrieves the submitted file(s), places them in a secure location behind the firewall for debugging and deletes them from the FTP site.

3.4 Methods for submission

Cal-PASS Plus member data submissions may be made in a number of ways: a) using the Cal-PASS Plus data validation software program, and submitted electronically via secure FTP technology (SFTP); or b) using the Cal-PASS Plus drag and drop loader, and submitted electronically via a Secure Socket Layer connection. At no time will Cal-PASS Plus accept member data submission files on disc, CD, DVD, or other media (i.e.: a flash drive).

3.5 Data Ownership and Use

All Cal-PASS Plus participants agree to adhere to the following data sharing guiding principles.

1. Data Ownership – Each school, community college and university retains the right to its own data. The sharing institutions can claim no right to ownership of data produced for research allowed via data sharing agreements. Moreover, institutional members of the sharing institutions are permitted access to data for uses that improve instruction and increase student success.

2. Data Uses - Information produced using Cal-PASS Plus data is *primarily* for internal institutional use.

3. Review for External Reporting – Every member will be contacted for approval before any data is externally released. Members will have the right to provide input on which data will be released and in what form.

4. Sensitivity to Members - Any reports utilizing Cal-PASS Plus data shall not disadvantage any member institution.

5. Confidentiality Safeguards - No individual person will be identified in any report. Each member will maintain as confidential all data received from any other member. Each party will establish at least the safeguards set forth in this guiding principle to ensure the continued confidentiality and security of the student data and to preclude the personal identification of students or their parties by persons other than designated officials of the institution. All student records will be kept in secure facilities. Any information published in any form by Cal-PASS Plus will not have the potential to identify individual students. Each institution will comply with all provisions of the Family Educational Rights and Privacy Act and applicable California law concerning the privacy of student records. The confidentiality requirements of this guiding principle shall survive termination or expiration of the data-sharing agreement/MOU. All student data transmitted to and retrieved from the Cal-PASS Plus server shall be maintained (processed, stored, and transmitted in a secure manner) to further protect the confidential nature of the data.

3.6 Personally Identifiable Information:

There is no personally identifiable information retained by Cal-PASS Plus or stored on the Cal-PASS Plus server. No names, addresses or Social Security Numbers are transmitted or stored by Cal-PASS Plus

4.0 Cal-PASS Plus Data Repository

4.1 Access to records (levels of access)

All access to Cal-PASS Plus data whether in unitary record format or in the aggregate is controlled with a User ID and password. When an MOU is signed (usually by a District Superintendent or College President), a Program Contact and IT contact are identified. User IDs and passwords can also be provided to verified users from the member institutions.

Login access to all Cal-PASS Plus servers is controlled by the full time SJDC Data Center and Cal-PASS Plus staff that have a signed confidentiality statement on file.

4.2 Physical security:

- Location: San Joaquin Delta College (SJDC) Data Center.
- Facility Front Door Entry: Secured by locking system that requires card access or code to open.
- Receptionist Area: Front Desk Receptionist with Sign In/Sign Out sheet.
- Server Room Entry: SJDC facility escort with badge security access to server room.
- Server Room Mantrap: Enclosed mantrap area that requires badge or code further entry into server room.
- Server Room Security Methods: Camera System and Server Rack intrusion sensors.
- Server Rack Entry: SJDC Data Center facility escort with 2 factor authentication including employee badge and keypad entry code.

4.3 Information security:

- Cal-PASS Plus data access is through a Secure Socket Layer (SSL) using DigiCert software.
- Documentation of the encryption routines used in the Cal-PASS Plus validation program is stored separate from the data. A firewall is in place and the routine is not disclosed.

- Identification of recipients of data is verified before transmission through DigiCert and passwords.

- Domain Login: Unique Identified Windows Login assigned by Systems Administrator through Active Directory.

- Username Policy: FirstInitialLastName@CalPASS.org

- Password Policy:
  - Minimum Password Length: 10 Characters
  - Password Complexity: Enabled
  - Password Requirements: Satisfy 3 of the following 4 categories.
    - English uppercase characters (A through Z)
    - English lowercase characters (a through z)
    - Base 10 Digits (0 through 9)
    - Non-alphabetic characters (!,$,#,%)
  - Password History: Enabled
  - Password Expiration: 60 days

- Domain Groups: Domain Users are assigned to Active Directory Security Groups to grant access to domain resources defined by the user's principle of least privilege.

- SQL Login: Domain Accounts assigned by Database Administrator to requested DB resources as defined by user's principle of least privilege.

- Encryption Software: Inline AES Encryption for Data-at-Rest

- Encryption Type: 256-bit AES encryption

- Encrypted Drive Volume Types: Bootable System Volume and Data Volumes.

- Backup Software: Windows Server Backup, SQL Server Backup

- Backup Schedule:
  Windows
  - Sunday-Saturday: Full Backup

  SQL
  - Sunday-Friday: Incremental DB and DB Logs Backup
  - Saturday: Full DB and DB Logs Backup

- Anti-Virus Software: Microsoft System Center Endpoint Protection

- Scheduled Scans: Saturday 2:00 AM

- Scheduled Definitions Update: Automatic

4.4 Records retention and destruction:

Currently, there are a maximum of 12 years of data in the Cal-PASS Plus system. When fully implemented, a rolling 17 years of data will be stored on the Cal-PASS Plus server. Records older than 17 years will be destroyed in accordance with the State of California protocols for destruction of electronic data.

4.5 Training:

- We provide Cal-PASS Plus employees with phishing training, FERPA training, and general IT protocol.

- Training is initially provided when new employees are onboarded and continued in response to an event.

- Materials for training include online tests for subjects such as FERPA, IASE, and security awareness issues like phishing attacks along with video examples on the same subjects.

- FERPA training through the University of Missouri is required for users who have access to SQL servers containing unitary student level records.

Appendix A

The Family Educational Right to Privacy Act (Buckley Amendment)
(as of 4/93)

20 USC S. 1232g

S. 1232g. Family educational and privacy rights

(a) Conditions for availability of funds to educational agencies or institutions; inspection and review of education records; specific information to be made available; procedure for access to education records; reasonableness of time for such access; hearings; written explanations by parents; definitions.

(1) (A) No funds shall be made available under any applicable program to any educational agency or institution which has a policy of denying, or which effectively prevents, the parents of students who are or have been in attendance at a school of such agency or at such institution, as the case may be, the right to inspect and review the education records of their children. If any material or document in the education record of a student includes information on more than one student, the parents of one of such students shall have the right to inspect and review only such part of such material or document as relates to such student or to be informed of the specific information contained in such part of such material. Each educational agency or institution shall establish appropriate procedures for the granting of a request by parents for access to the education records of their children within a reasonable period of time, but in no case more than forty-five days after the request has been made.

(B) The first sentence of subparagraph (A) shall not operate to make available to students in institutions of postsecondary education the following materials:

(i) financial records of the parents of the student or any information contained therein;
(ii) confidential letters and statements of recommendation, which were placed in the education records prior to January 1, 1975, if such letters or statements are not used for purposes other than those for which they were specifically intended;
(iii) if the student has signed a waiver of the student's right of access under this subsection in accordance with subparagraph (C), confidential recommendations--

(I) respecting admission to any educational agency or institution,

(II) respecting an application for employment, and

(III) respecting the receipt of an honor or honorary recognition.

(C) A student or a person applying for admission may waive his right of access to confidential statements described in clause (iii) of subparagraph (B), except that such waiver shall apply to recommendations only if (i) the student is, upon request, notified of the names of all persons making confidential recommendations and (ii) such recommendations are used solely for the purpose for which they were specifically intended. Such waivers may not be required as a condition for admission to, receipt of financial aid from, or receipt of any other services or benefits from such agency or institution.

(2) No funds shall be made available under any applicable program to any educational agency or institution unless the parents of students who are or have been in attendance at a school of such agency or at such institution are provided an opportunity for a hearing by such agency or institution, in accordance with regulations of the Secretary, to challenge the content of such student's education records, in order to insure that the records are not inaccurate, misleading, or otherwise in violation of the privacy or other rights of students, and to provide an opportunity for the correction or deletion of any such inaccurate, misleading, or otherwise inappropriate data contained therein and to insert into such records a written explanation of the parents respecting the content of such records.

(3) For the purposes of this section the term "educational agency or institution" means any public or private agency or institution which is the recipient of funds under any applicable program.

(4) (A) For the purposes of this section, the term "education records" means, except as may be provided otherwise in subparagraph (B), those records, files, documents, and other materials which--

(i) contain information directly related to a student; and

(ii) are maintained by an educational agency or institution or by a person acting for such agency or institution.

(B) The term "education records" does not include--

(i) records of instructional, supervisory, and administrative personnel and educational personnel ancillary thereto which are in the sole possession of the maker thereof and which are not accessible or revealed to any other person except a substitute;

(ii) records maintained by a law enforcement unit of the educational agency or institution that were created by that law enforcement unit for the purpose of law enforcement.

(iii) in the case of persons who are employed by an educational agency or institution but who are not in attendance at such agency or institution, records made and maintained in the normal course of business which relate exclusively to such person in

that person's capacity as an employee and are not available for use for any other purpose; or

(iv) records on a student who is eighteen years of age or older, or is attending an institution of postsecondary education, which are made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in his professional or paraprofessional capacity, or assisting in that capacity, and which are made, maintained, or used only in connection with the provision of treatment to the student, and are not available to anyone other than persons providing such treatment, except that such records can be personally reviewed by a physician or other appropriate professional of the student's choice.

(5) (A) For the purposes of this section the term "directory information" relating to a student includes the following: the student's name, address, telephone listing, date and place of birth, 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, and the most recent previous educational agency or institution attended by the student.

(B) Any educational agency or institution making public directory information shall give public notice of the categories of information which it has designated as such information with respect to each student attending the institution or agency and shall allow a reasonable period of time after such notice has been given for a parent to inform the institution or agency that any or all of the information designated should not be released without the parent's prior consent.

(6) For the purposes of this section, the term "student" includes any person with respect to whom an educational agency or institution maintains education records or personally identifiable information, but does not include a person who has not been in attendance at such agency or institution.

(b) Release of education records; parental consent requirement; exceptions; compliance with judicial orders and subpoenas; audit and evaluation of Federally-supported education programs; recordkeeping.

(1) No funds shall be made available under any applicable program to any educational agency or institution which has a policy or practice of permitting the release of educational records (or personally identifiable information contained therein other than directory information, as defined in paragraph (5) of subsection (a)) of students without the written consent of their parents to any individual, agency, or organization, other than to the following--

(A) other school officials, including teachers within the educational institution or local educational agency, who have been determined by such agency or institution to have legitimate educational interests;

(B) officials of other schools or school systems in which the student seeks or intends to enroll, upon condition that the student's parents be notified of the transfer, receive a copy of the record if desired, and have an opportunity for a hearing to challenge the content of the record;

(C) authorized representatives of (i) the Comptroller General of the United States, (ii) the Secretary, (iii) an administrative head of an educational agency (as defined in section 408(c) , or (iv) State educational authorities, under the conditions set forth in paragraph (3) of this subsection;

(D) in connection with a student's application for, or receipt of, financial aid;

(E) State and local officials or authorities to whom such information is specifically required to be reported or disclosed pursuant to State statute adopted prior to November 19, 1974;

(F) organizations conducting studies for, or on behalf of, educational agencies or institutions for the purpose of developing, validating, or administering predictive tests, administering student aid programs, and improving instruction, if such studies are conducted in such a manner as will not permit the personal identification of students and their parents by persons other than representatives of such organizations and such information will be destroyed when no longer needed for the purpose for which it is conducted;

(G) accrediting organizations in order to carry out their accrediting functions;

(H) parents of a dependent student of such parents, as defined in section 152 of the Internal Revenue Code of 1954; and

(I) subject to regulations of the Secretary, in connection with an emergency, appropriate persons if the knowledge of such information is necessary to protect the health or safety of the student or other persons

Nothing in clause (E) of this paragraph shall prevent a State from further limiting the number or type of State or local officials who will continue to have access thereunder.

(2) No funds shall be made available under any applicable program to any educational agency or institution which has a policy or practice of releasing, or providing access to, any personally identifiable information in education records other than directory information, or as is permitted under paragraph (1) of this subsection unless--

(A) there is written consent from the student's parents specifying records to be released, the reasons for such release, and to whom, and with a copy of the records to be released to the student's parents and the student if desired by the parents, or

(B) such information is furnished in compliance with judicial order, or pursuant to any lawfully issued subpoena, upon condition that parents and the students are notified of all such orders or subpoenas in advance of the compliance therewith by the educational institution or agency.

(3) Nothing contained in this section shall preclude authorized representatives of (A) the Comptroller General of the United States, (B) the Secretary, (C) an administrative head of an education agency or (D) State educational authorities from having access to student or other records which may be necessary in connection with the audit and evaluation of Federally-supported education program, or in connection with the enforcement of the Federal legal requirements which relate to such programs: Provided, That except when collection of personally identifiable information is specifically authorized by Federal law, any data collected by such officials shall be protected in a manner which will not permit the personal identification of students and their parents by other than those officials, and such personally identifiable data shall be destroyed when no longer needed for such audit, evaluation, and enforcement of Federal legal requirements.

(4) (A) Each educational agency or institution shall maintain a record, kept with the education records of each student, which will indicate all individuals (other than those specified in paragraph (1) (A) of this subsection), agencies, or organizations which have requested or obtained access to a student's education records maintained by such educational agency or institution, and which will indicate specifically the legitimate interest that each such person, agency, or organization has in obtaining this information. Such record of access shall be available only to parents, to the school official and his assistants who are responsible for the custody of such records, and to persons or organizations authorized in, and under the conditions of, clauses (A) and (C) of paragraph (1) as a means of auditing the operation of the system.

(B) With respect to this subsection, personal information shall only be transferred to a third party on the condition that such party will not permit any other party to have access to such information without the written consent of the parents of the student.

(5) Nothing in this section shall be construed to prohibit State and local educational officials from having access to student or other records which may be necessary in connection with the audit and evaluation of any federally or State supported education program or in connection with the enforcement of the Federal legal requirements which relate to any such program, subject to the conditions specified in the proviso in paragraph (3).

(6) Nothing in this section shall be construed to prohibit an institution of postsecondary education from disclosing, to an alleged victim of any crime of violence (as that term is defined in section 16 of title 18, United States Code), the results of any disciplinary proceeding conducted by such institution against the alleged perpetrator of such crime with respect to such crime.

(c) Surveys or data-gathering activities; regulations. The Secretary shall adopt appropriate regulations to protect the rights of privacy of students and their families in connection with any surveys or data-gathering activities conducted, assisted, or authorized by the Secretary or an administrative head of an education agency. Regulations established under this subsection shall include provisions controlling the use, dissemination, and protection of such data. No survey or data-gathering activities shall be conducted by the Secretary, or an administrative head of an education agency under an applicable program, unless such activities are authorized by law.

(d) Students' rather than parents' permission or consent. For the purposes of this section, whenever a student has attained eighteen years of age, or is attending an institution of postsecondary education the permission or consent required of and the rights accorded to the parents of the student shall thereafter only be required of and accorded to the student.

(e) Informing parents or students of rights under this section. No funds shall be made available under any applicable program to any educational agency or institution unless such agency or institution informs the parents of students, or the students, if they are eighteen years of age or older, or are attending an institution of postsecondary education, of the rights accorded them by this section.

(f) Enforcement; termination of assistance. The Secretary, or an administrative head of an education agency, shall take appropriate actions to enforce provisions of this section and to deal with violations of this section, according to the provisions of this Act, except that action to terminate assistance may be taken only if the Secretary finds there has been a failure to comply with the provisions of this section, and he has determined that compliance cannot be secured by voluntary means.

(g) Office and review board; creation; functions. The Secretary shall establish or designate an office and review board within the Department of Health, Education, and Welfare for the purpose of investigating, processing, reviewing, and adjudicating violations of the provisions of this section and complaints which may be filed concerning alleged violations of this section. Except for the conduct of hearings, none of the functions of the Secretary under this section shall be carried out in any of the regional offices of such Department.