Student Privacy Protection Agreement:

California Assembly Bill 1584 Agreement Template

This Agreement is entered into between District Azusa Unified Local Education Agency ("LEA") and the Foundation for California Community Colleges ("FOUNDATION"), as it relates to LEA's intended use of www.CaliforniaColleges.edu (also referred to herein as "Website"), on 7th day of February, 2023 ("Effective Date".)

WHEREAS, FOUNDATION has entered into an agreement with MaiaLearning, Inc. ("Service Provider") for technology services which are provided at www.CaliforniaColleges.edu and Service Provider has confirmed, in the agreement, its compliance with California Assembly Bill 1584 ("AB 1584"), as further outlined below;

WHEREAS, the LEA is a California public entity subject to all state and federal laws governing education, including but not limited to AB 1584, the California Education Code, the Children's Online Privacy and Protection Act ("COPPA"), and the Family Educational Rights and Privacy Act ("FERPA");

WHEREAS, the LEA has advised the FOUNDATION that they wish to use the Website with their pupils and FOUNDATION, as the sponsor of the Website has agreed to such use by LEA;

WHEREAS, AB 1584 requires, in part, that any agreement entered into, renewed or amended after January 1, 2015, between a local education agency and a third-party service provider must include certain terms; and

WHEREAS, the LEA and FOUNDATION desire to have the services available to the LEA at www.CaliforniaColleges.edu comply with AB 1584.

NOW, THEREFORE, the Parties agree as follows:

1. The terms and conditions of this Agreement together with the Website Terms of Use and Privacy Policy, current versions of which are posted at www.CaliforniaColleges.edu, shall govern use of the Website by the LEA and their students.

2. Pupil records entered into accounts on the Website by students of the LEA shall continue to be the property of, and under the control of, the LEA.

3. The procedures by which students may retain possession and control of or transfer to a personal account, their own student-generated content are outlined as follows:
   a) LEA will advise FOUNDATION that it plans to cease use of the website with its pupils and terminate this Agreement;
   b) If LEA is not intending to request that Service Provider delete all LEA pupil accounts, LEA will advise students they may continue to use their pupil-generated account as they wish, under their own direction.

4. Parents, legal guardians, or eligible students may review personally identifiable information in their child(ren)'s records and correct erroneous information by the following protocol:
   a) Student uses the "Invite a Parent or Guardian to access your portfolio" functionality on the Website to invite their parent or legal guardian to view their portfolio;

b) Parent reviews the portfolio and identifies any student-generated information that requires correction;
c) Parent works with their child(ren) to log on to their portfolio and edit the information they have entered, if editable;
d) If not editable, parent may contact the Service Provider, at the contact information provided in the "Modifying and Deleting Your Information" section of the Website Privacy Policy, to request that the erroneous information be corrected or deleted.

5. Service Provider has taken action and implemented procedures to ensure the security and confidentiality of pupil records, including but not limited to designating and training responsible individuals on ensuring the security and confidentiality of pupil records by the following measures:
   a) All pupil records are stored in Service Provider's highly secured data center with 24/7onsite security and biometric access control.
   b) All of Service Provider's servers are protected by state-of-the-art firewall systems and monitoring alerts in multiple levels for monitoring any unusual activity. Dedicated personnel actively monitor activity and adjust firewalls in anticipation of potential threats.
   c) All pupil data/records entered on the Website are encrypted when on route between the user's browser and Service Provider's servers and when on route between the servers and another browser or server. This prevents unauthorized third parties from intercepting and gaining access to pupil data during transmission over the Internet. Service Provider uses 128-bit, Secure Socket Layer (SSL) encryption supported by all common browsers.
   d) Access to all pupil data requires authentication using personal usernames and passwords.
   e) Service Provider staff members would only access pupil data for support purposes and only do so at the request of the LEA or the student, and their access is authenticated using personal usernames and passwords.

6. In addition to requiring that Service Provider ensures the security and confidentiality of pupil records, FOUNDATION shall maintain policies and procedures for the designation and training of responsible staff members to ensure the confidentiality and security of Student Data.
   f) The FOUNDATION provides data security and privacy training upon hire and on an annual basis to its staff members who work with Student Data. The training covers Federal, State, and Local regulations for maintenance of student data, as well as best practices.
   g) At LEA's request, FOUNDATION shall provide LEA with contact information of an employee who LEA may contact if there are any security concerns or questions.
   h) FOUNDATION access to pupil records requires authentication using unique personal usernames and passwords.
   i) FOUNDATION will not access pupil records outside of the Service Provider's highly controlled platform, described in Section 6 above.

7. In the event of an unauthorized disclosure of a pupil's records, Service Provider shall report toan affected parent, legal guardian, or eligible student pursuant to the following procedure:
   j) Service Provider will contact the LEA signatory to this Agreement to advise ofthe unauthorized disclosure of the pupil's records;
   k) Service Provider will work with the LEA with regard to mitigation efforts related tothe disclosure and notification to the parents or legal guardian of the affected pupil.

l) If requested by LEA in agreement with the parents or legal guardian of the affected pupil and the pupil, Service Provider will delete pupil's student-generated account.

8. FOUNDATION certifies that the Foundation and its Service Provider shall not use any information in a pupil record for any purpose other than those required or specifically permitted by the Website Terms of Use and Privacy Policy. More particularly, the Foundation and its Service Provider will not use personally identifiable information in pupil records to engage in targeted advertising.

9. FOUNDATION certifies that a pupil's records shall not be retained or available to the Foundation or its Service Provider upon completion of the LEA's use of the Website, so long as the LEA notifies the FOUNDATION and Service Provider of their intention to cease use of the Website and the LEA provides to the Service Provider, by secure means, a list of all pupil account names that they require to be deleted; except for a case where a pupil chooses to establish or maintain an account with Service Provider for the purpose of storing pupil-generated content, either by retaining possession and control of their own pupil- generated content, or by transferring pupil generated content to a personal account. Such certification will be enforced through the following procedure:
   m) LEA notifies FOUNDATION that they will cease using the Website with their students and wish to terminate this Agreement.
   n) LEA, through the Professional Tools offered on the Website will download and provide to the Service Provider, by secure means, a list of all student accounts to be deleted.
   o) Service Provider will delete the accounts and notify the LEA that the accounts have been deleted.

10. LEA agrees to comply with FERPA in directing their students' use of the Website. FOUNDATION and Service Provider's compliance with FERPA is confirmed in the Website Privacy Policy.

11. LEA agrees to the Data Privacy and Security Addendum attached hereto as Exhibit A, which contains information about the redisclosure of data under this Agreement.

IN WITNESS WHEREOF, parties execute this Agreement on the dates set forth below.

District Azusa Unified School District

By: _____

Print Name: Arturo Ortega

Title: Superintendent

Date: 2/7/2023

FOUNDATION FOR CALIFORNIA COMMUNITY COLLEGES

By: _____

Print Name: Tessa Carmen De Roy

Title: President, CCGI

Date: 8/8/2022

EXHIBIT A

DATA PRIVACY AND SECURITY ADDENDUM

The purpose of this addendum is to provide a more detailed review of federal and state data privacy and security compliance measures that apply to this Partnership Agreement, specifically addressing the requirements of the Family Educational Rights and Privacy Act ("FERPA"), the Children's Online Privacy Protection Act of 1998 ("COPPA"), California Education Code Section 49073.1, commonly referred to as California Assembly Bill 1584 (or "AB 1584"), and California Business and Professions Code Section 22584, commonly referred to as the "Student Online Personal Information Protection Act" (or "SOPIPA") or "SB 1177".

The Foundation for California Community Colleges ("Foundation"), on behalf of its fiscally sponsored project, the California College Guidance Initiative ("CCGI"), receives public funding via the state of California, for the purpose of developing, operating, and maintaining the CaliforniaColleges Website. Foundation, on behalf of CCGI, sub-contracts with a third party vendor ("Vendor") to perform the development, operation, and maintenance work. Foundation staff perform data analysis, LEA support, and serve as the direct point of contact for CaliforniaColleges Website users, as well as manage data sharing relationships and technological articulations with institutions of higher education and financial aid providers.

Foundation Contact for Data Privacy and Security Inquiries
Leigh Ranck
Chief Technology Officer
California College Guidance Initiative
Foundation for California Community Colleges
1102 Q Street, Suite 4800
Sacramento, CA 95811
lranck@californiacolleges.org

I. DATA COLLECTION

A. Foundation, on behalf of CCGI, collects the following information from LEA and/or directly from its students ("System Users"):

1. Via LEA electronic transcript file:
   a) LEA demographic data
   b) Student demographic data
   c) Student course data
   d) Student test data
   e) Student ethnicity data
2. Via CaliforniaColleges.edu:
   a) Student-generated data resulting from college and career planning activities like college lists, career lists, major lists, and career assessment results.

B. Education Records, including Student Data, collected from the LEA continue to be the property of and under the control of the LEA.

C. Upon termination the agreement between LEA and the Foundation, System Users will be provided notification and instructions on steps to take in order retain possession and control of their own student-generated data, if applicable.

D. Unless a System User elects to maintain their CaliforniaColleges Website account, any Student Data uploaded by LEA will not be retained or available to Foundation or any third party upon termination of this agreement.

II. DATA USE

A. The information listed above is used to create student portfolios on the CaliforniaColleges Website for use in college and career planning and guidance activities.

B. Education Records, including Student Data, may only be used as specifically required or permitted by this agreement or in the terms of use and privacy policy on CaliforniaColleges.edu.

C. Foundation shall not sell, use or permit any third party to use Student Data, including PII, for commercial purposes or for targeted advertising.

III. WHO HAS ACCESS TO DATA (AUTHORIZED DISCLOSURES)

A. The information from student's portfolios may be disclosed to the officials or employees of the following groups who have a legitimate interest in the information for purposes consistent with this agreement:

1. Foundation/CCGI (collects and maintains Student Data).
2. Vendor (maintains Student Data).
3. CaliforniaColleges Website and FTP infrastructure (will not access or use content for any purpose other than as legally required and for maintaining services, and will not directly process or access content).
4. Any College or College System to which a System User has applied for admission (can be provided Student Data for the purposes of admission, enrollment, matriculation, placement and supportive services).
5. Any Financial Aid Organization to which a System User has applied for aid, or with whom the LEA has legally shared Student Data under California law, including, but not limited to, the California Student Aid Commission ("CSAC").
    a) Under California Education Code §69432.9 LEAs are generally required to provide and verify their student's grade point average to the CSAC for the Cal Grant Program application. The Foundation, on behalf of CCGI, and the CSAC may provide PII to CSAC to support CSAC's data matching process by providing CSAC data elements that help to associate the correct SSID with the student's FAFSA if it is launched via the CaliforniaColleges.edu platform. This data matching assistance helps to facilitate the determination of Cal Grant Program eligibility for students who attend and graduate from a LEA.
6. The LEA's County Office of Education for the purpose of assisting in planning or preparing for college or a career, seeking admission to college or financial aid for college, and/or research and analysis to help improve instruction and student success.
7. Foundation may provide Student Data in an aggregated, non-personally identifiable form, to other contracted entities for the purpose of evaluating the impact and effectiveness of the CCGI program.

B. The Parties shall maintain policies and procedures for the designation and training of responsible staff members to ensure the confidentiality and security of Student Data. The Foundation provides data security and privacy training on an annual basis to CCGI staff handling student data. The training covers Federal, State, and Local regulations for maintenance of student data, as well as best practices. All new staff undergo data security and privacy training prior to gaining access to CaliforniaColleges.edu. All data is encrypted both at rest and during transmission using commercially reasonable practices.