

CALIFORNIA STUDENT DATA PRIVACY
AGREEMENT Version 2.0 (September 26, 2018)

School District/Local Education Agency:

San Joaquin County Office of Education

AND

Provider:

Early Quality Systems-Hubbe Inc.

Date:

05-21-2021

This California Student Data Privacy Agreement (“DPA”) is entered into by and between the San Joaquin County Office of Education

(hereinafter referred to as “LEA”) and Early Quality Systems-Hubbe Inc. (hereinafter referred to as “Provider”) on 05-21-2021 . The Parties agree to the terms as stated herein.

RECITALS

WHEREAS, the Provider has agreed to provide the Local Education Agency (“LEA”) with certain digital educational services (“Services”) pursuant to a contract dated (“Service Agreement”); and

05-21-2021

WHEREAS, in order to provide the Services described in the Service Agreement, the Provider may receive or create, and the LEA may provide documents or data that are covered by several federal statutes, among them, the Family Educational Rights and Privacy Act (“FERPA”) at 20 U.S.C. 1232g (34 CFR Part 99), Children’s Online Privacy Protection Act (“COPPA”), 15 U.S.C. 6501-6506; Protection of Pupil Rights Amendment (“PPRA”) 20 U.S.C. 1232h; and

WHEREAS, the documents and data transferred from LEAs and created by the Provider’s Services are also subject to California state student privacy laws, including AB 1584, found at California Education Code Section 49073.1 and the Student Online Personal Information Protection Act (“SOPIPA”) found at California Business and Professions Code section 22584; and

WHEREAS, for the purposes of this DPA, Provider is a school official with legitimate educational interests in accessing educational records pursuant to the Service Agreement; and

WHEREAS, the Parties wish to enter into this DPA to ensure that the Service Agreement conforms to the requirements of the privacy laws referred to above and to establish implementing procedures and duties; and

WHEREAS, the Provider may, by signing the “General Offer of Privacy Terms” (Exhibit “E”), agree to allow other LEAs in California the opportunity to accept and enjoy the benefits of this DPA for the Services described herein, without the need to negotiate terms in a separate DPA.

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA.** The purpose of this DPA is to describe the duties and responsibilities to protect student data transmitted to Provider from LEA pursuant to the Service Agreement, including compliance with all applicable statutes, including the FERPA, PPRA, COPPA, SOPIPA, AB 1584, and other applicable California State laws, all as may be amended from time to time. In performing these services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. With respect to the use and maintenance of Student Data, Provider shall be under the direct control and supervision of the LEA.

2. **Nature of Services Provided.** The Provider has agreed to provide the following digital educational products and services described below and as may be further outlined in Exhibit "A" hereto:

QRIS Hubbe located at: SJCOE.iPinwheel.org

3. **Student Data to Be Provided.** The Parties shall indicate the categories of student data to be provided in the Schedule of Data, attached hereto as Exhibit "B".
4. **DPA Definitions.** The definition of terms used in this DPA is found in Exhibit "C". In the event of a conflict, definitions used in this DPA shall prevail over term used in the Service Agreement.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA.** All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this Agreement in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEAs as it pertains to the use of Student Data notwithstanding the above. Provider may transfer pupil-generated content to a separate account, according to the procedures set forth below.
2. **Parent Access.** LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Student Data in the pupil's records, correct erroneous information, and procedures for the transfer of pupil-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a timely manner (and no later than 45 days from the date of the request) to the LEA's request for Student Data in a pupil's records held by the Provider to view or correct as necessary. In the event that a parent of a pupil or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.
3. **Separate Account.** If pupil generated content is stored or maintained by the Provider as part of the Services described in Exhibit "A", Provider shall, at the request of the LEA, transfer said pupil generated content to a separate student account upon termination of the Service Agreement; provided, however, such transfer shall only apply to pupil generated content that is severable from the Service.
4. **Third Party Request.** Should a Third Party, including law enforcement and government entities, contact Provider with a request for data held by the Provider pursuant to the Services, the Provider shall redirect the Third Party to request the data directly from the LEA. Provider shall notify the LEA in advance of a compelled disclosure to a Third Party.

5. **Subprocessors**. Provider shall enter into written agreements with all Subprocessors performing functions pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in manner consistent with the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Privacy Compliance**. LEA shall provide data for the purposes of the Service Agreement in compliance with FERPA, COPPA, PPRRA, SOPIPA, AB 1584 and all other California privacy statutes.
2. **Annual Notification of Rights**. If the LEA has a policy of disclosing education records under FERPA (4 CFR § 99.31 (a) (1)), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its Annual notification of rights.
3. **Reasonable Precautions**. LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted data.
4. **Unauthorized Access Notification**. LEA shall notify Provider promptly of any known or suspected unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance**. The Provider shall comply with all applicable state and federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRRA, SOPIPA, AB 1584 and all other California privacy statutes.
2. **Authorized Use**. The data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services stated in the Service Agreement and/or otherwise authorized under the statutes referred to in subsection (1), above. Provider also acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, meta data, user content or other non-public information and/or personally identifiable information contained in the Student Data, without the express written consent of the LEA.
3. **Employee Obligation**. Provider shall require all employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the data shared under the Service Agreement.
4. **No Disclosure**. De-identified information may be used by the Provider for the purposes of development, research, and improvement of educational sites, services, or applications, as any other member of the public or party would be able to use de-identified data pursuant to 34 CFR 99.31(b). Provider agrees not to attempt to re-identify de-identified Student Data and not to transfer de-identified Student Data to any party unless (a) that party agrees in writing not to

attempt re-identification, and (b) prior written notice has been given to LEA who has provided prior written consent for such transfer. Provider shall not copy, reproduce or transmit any data obtained under the Service Agreement and/or any portion thereof, except as necessary to fulfill the Service Agreement.

5. **Disposition of Data.** Upon written request and in accordance with the applicable terms in subsection a or b, below, Provider shall dispose or delete all Student Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained. Disposition shall include (1) the shredding of any hard copies of any Student Data; (2) Erasing; or (3) Otherwise modifying the personal information in those records to make it unreadable or indecipherable by human or digital means. Nothing in the Service Agreement authorizes Provider to maintain Student Data obtained under the Service Agreement beyond the time period reasonably needed to complete the disposition. Provider shall provide written notification to LEA when the Student Data has been disposed. The duty to dispose of Student Data shall not extend to data that has been de-identified or placed in a separate Student account, pursuant to the other terms of the DPA. The LEA may employ a “Request for Return or Deletion of Student Data” form, a copy of which is attached hereto as Exhibit “D”. Upon receipt of a request from the LEA, the Provider will immediately provide the LEA with any specified portion of the Student Data within ten (10) calendar days of receipt of said request.
 - a. **Partial Disposal During Term of Service Agreement.** Throughout the Term of the Service Agreement, LEA may request partial disposal of Student Data obtained under the Service Agreement that is no longer needed. Partial disposal of data shall be subject to LEA’s request to transfer data to a separate account, pursuant to Article II, section 3, above.
 - b. **Complete Disposal Upon Termination of Service Agreement.** Upon Termination of the Service Agreement Provider shall dispose or delete all Student Data obtained under the Service Agreement. Prior to disposition of the data, Provider shall notify LEA in writing of its option to transfer data to a separate account, pursuant to Article II, section 3, above. In no event shall Provider dispose of data pursuant to this provision unless and until Provider has received affirmative written confirmation from LEA that data will not be transferred to a separate account.
6. **Advertising Prohibition.** Provider is prohibited from using or selling Student Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing, advertising, or other commercial efforts by a Provider; (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Service to LEA; or (d) use the Student Data for the development of commercial products or services, other than as necessary to provide the Service to LEA. This section does not prohibit Provider from using Student Data for adaptive learning or customized student learning purposes.

ARTICLE V: DATA PROVISIONS

1. **Data Security.** The Provider agrees to abide by and maintain adequate data security measures, consistent with industry standards and technology best practices, to protect Student Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of

Provider are set forth below. Provider may further detail its security programs and measures in Exhibit "F" hereto. These measures shall include, but are not limited to:

- a. **Passwords and Employee Access.** Provider shall secure usernames, passwords, and any other means of gaining access to the Services or to Student Data, at a level suggested by the applicable standards, as set forth in Article 4.3 of NIST 800-63-3. Provider shall only provide access to Student Data to employees or contractors that are performing the Services. Employees with access to Student Data shall have signed confidentiality agreements regarding said Student Data. All employees with access to Student Records shall be subject to criminal background checks in compliance with state and local ordinances.
- b. **Destruction of Data.** Provider shall destroy or delete all Student Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained, or transfer said data to LEA or LEA's designee, according to the procedure identified in Article IV, section 5, above. Nothing in the Service Agreement authorizes Provider to maintain Student Data beyond the time period reasonably needed to complete the disposition.
- c. **Security Protocols.** Both parties agree to maintain security protocols that meet industry standards in the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. Provider shall maintain all data obtained or generated pursuant to the Service Agreement in a secure digital environment and not copy, reproduce, or transmit data obtained pursuant to the Service Agreement, except as necessary to fulfill the purpose of data requests by LEA.
- d. **Employee Training.** The Provider shall provide periodic security training to those of its employees who operate or have access to the system. Further, Provider shall provide LEA with contact information of an employee who LEA may contact if there are any security concerns or questions.
- e. **Security Technology.** When the service is accessed using a supported web browser, Provider shall employ industry standard measures to protect data from unauthorized access. The service security measures shall include server authentication and data encryption. Provider shall host data pursuant to the Service Agreement in an environment using a firewall that is updated according to industry standards.
- f. **Security Coordinator.** If different from the designated representative identified in Article VII, section 5, Provider shall provide the name and contact information of Provider's Security Coordinator for the Student Data received pursuant to the Service Agreement.
- g. **Subprocessors Bound.** Provider shall enter into written agreements whereby Subprocessors agree to secure and protect Student Data in a manner consistent with the terms of this Article V. Provider shall periodically conduct or review compliance

monitoring and assessments of Subprocessors to determine their compliance with this Article.

- h. Periodic Risk Assessment.** Provider further acknowledges and agrees to conduct digital and physical periodic (no less than semi-annual) risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner.

2. Data Breach. In the event that Student Data is accessed or obtained by an unauthorized individual, Provider shall provide notification to LEA within a reasonable amount of time of the incident, and not exceeding forty-eight (48) hours. Provider shall follow the following process:

- a.** The security breach notification shall be written in plain language, shall be titled “Notice of Data Breach,” and shall present the information described herein under the following headings: “What Happened,” “What Information Was Involved,” “What We Are Doing,” “What You Can Do,” and “For More Information.” Additional information may be provided as a supplement to the notice.
- b.** The security breach notification described above in section 2(a) shall include, at a minimum, the following information:
 - i.** The name and contact information of the reporting LEA subject to this section.
 - ii.** A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
 - iii.** If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
 - iv.** Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.
 - v.** A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
- c.** At LEA’s discretion, the security breach notification may also include any of the following:
 - i.** Information about what the agency has done to protect individuals whose information has been breached.
 - ii.** Advice on steps that the person whose information has been breached may take to protect himself or herself.
- d.** Provider agrees to adhere to all requirements in applicable State and in federal law with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.

- e. Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a copy of said written incident response plan.
- f. Provider is prohibited from directly contacting parent, legal guardian or eligible pupil unless expressly requested by LEA. If LEA requests Provider's assistance providing notice of unauthorized access, and such assistance is not unduly burdensome to Provider, Provider shall notify the affected parent, legal guardian or eligible pupil of the unauthorized access, which shall include the information listed in subsections (b) and (c), above. If requested by LEA, Provider shall reimburse LEA for costs incurred to notify parents/families of a breach not originating from LEA's use of the Service.
- g. In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

ARTICLE VI- GENERAL OFFER OF PRIVACY TERMS

Provider may, by signing the attached Form of General Offer of Privacy Terms (General Offer, attached hereto as Exhibit "E"), be bound by the terms of this DPA to any other LEA who signs the acceptance on in said Exhibit. The Form is limited by the terms and conditions described therein.

ARTICLE VII: MISCELLANEOUS

1. **Term.** The Provider shall be bound by this DPA for the duration of the Service Agreement or so long as the Provider maintains any Student Data. .
2. **Termination.** In the event that either party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. LEA shall have the right to terminate the DPA and Service Agreement in the event of a material breach of the terms of this DPA.
3. **Effect of Termination Survival.** If the Service Agreement is terminated, the Provider shall destroy all of LEA's data pursuant to Article V, section 1(b), and Article II, section 3, above.
4. **Priority of Agreements.** This DPA shall govern the treatment of student data in order to comply with privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the DPA and the Service Agreement, the DPA shall apply and take precedence. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.
5. **Notice.** All notices or other communication required or permitted to be given hereunder must be in writing and given by personal delivery, or e-mail transmission (if contact information is

provided for the specific mode of delivery), or first-class mail, postage prepaid, sent to the designated representatives before:

a. Designated Representatives

The designated representative for the LEA for this Agreement is:

Name: Jamie Baiocchi
Title: Div. Dir., Early Education & Support

Contact Information:
San Joaquin County Office of Education
PO Box 213030
Stockton, CA 95213-9030

The designated representative for the Provider for this Agreement is:

Name: Claire Crandall
Title: Director

Contact Information:
Claire@iPinwheel.com
Claire@Hubbeinc.com
760-644-4922

b. Notification of Acceptance of General Offer of Terms. Upon execution of Exhibit E, General Offer of Terms, Subscribing LEA shall provide notice of such acceptance in writing and given by personal delivery, or e-mail transmission (if contact information is provided for the specific mode of delivery), or first-class mail, postage prepaid, to the designated representative below.

The designated representative for the notice of acceptance of the General Offer of Privacy Terms is:

Name: Claire Crandall
Title: Director

Contact Information:
Claire@iPinwheel.com
Claire@Hubbeinc.com
760-644-4922

6. **Entire Agreement.** This DPA constitutes the entire agreement of the parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and

either retroactively or prospectively) only with the signed written consent of both parties. Neither failure nor delay on the part of any party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.

7. **Severability**. Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.
8. **Governing Law; Venue and Jurisdiction**. THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE IN WHICH THIS AGREEMENT IS EXECUTED, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY IN WHICH THIS AGREEMENT IS FORMED FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS SERVICE AGREEMENT OR THE TRANSACTIONS CONTEMPLATED HEREBY.
9. **Authority**. Provider represents that it is authorized to bind to the terms of this Agreement, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof, or may own, lease or control equipment or facilities of any kind where the Student Data and portion thereof stored, maintained or used in any way. Provider agrees that any purchaser of the Provider shall also be bound to the Agreement.
10. **Waiver**. No delay or omission of the LEA to exercise any right hereunder shall be construed as a waiver of any such right and the LEA reserves the right to exercise any such right from time to time, as often as may be deemed expedient.
11. **Successors Bound**. This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business.

[Signature Page Follows]

IN WITNESS WHEREOF, the parties have executed this California Student Data Privacy Agreement as of the last day noted below.

Provider: Early Quality Systems-Hubbe Inc.

BY:  Date: 6/9/2021

Printed Name: Claire Crandall Title/Position: Director

Local Education Agency: San Joaquin County Office of Education

BY:  Date: 6-26-2021

Printed Name: Jamie Baiocchi Title/Position: Div. Dir., Early Education & Support

 6/16/21

Note: Electronic signature not permitted.

EXHIBIT "A"

DESCRIPTION OF SERVICES

[INSERT DETAILED DESCRIPTION OF PRODUCTS AND SERVICES HERE. IF MORE THAN ONE PRODUCT OR SERVICE IS INCLUDED, LIST EACH PRODUCT HERE]

Early Quality Systems-Hubbe Inc. operates the Early Childhood Integrated Data System (ECIDS) called iPinwheel-Hubbe. The Quality Rating and Improvement System component of the Early Childhood Integrated Data System is called The QRIS Hubbe. The QRIS Hubbe is a browser-based web application with a centralized database that tracks, measures, stores, and reports the data needed to implement and manage a successful large-scale QRIS to improve the quality of early childhood education. QRIS Hubbe California has been specifically designed to support agencies to successfully administer their Quality Counts California State – funded QRIS program and report the outcomes to the California Department of Education and to First 5 California, the program funder. The system can also be used to manage successfully manage and report on the state-funded Workforce Pathways Grant.

The QRIS Hubbe California system provides an easy-to-use graphical user interface (GUI) available via browsers on popular computing platforms such as PCs, iPads, and Mobile devices. The system can be securely accessed anytime anywhere via the Internet using the internet browser Google Chrome. Having a browser-based solution that is a Server-Side Application, rather than a Client-Side Application, means that the application is delivered from the server to the browser, and does not reside as an application on each individual computer. In this manner, no special client software or installations are required. When QRIS Hubbe California is updated at the server, it is immediately available to all users.

EXHIBIT "B"

SCHEDULE OF DATA

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	X
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	X
Assessment	Standardized test scores	
	Observation data	X
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications that are captured (emails, blog entries)	X

Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, preferred or primary language spoken by student)	
	Other demographic information-Please specify:	
Enrollment	Student school enrollment	
	Student grade level	
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	X
	Year of graduation	
	Other enrollment information-Please specify:	
Parent/Guardian Contact Information	Address	
	Email	
	Phone	

Parent/ Guardian ID	Parent ID number (created to link parents to students)	
Parent/ Guardian Name	First and/or Last	
Schedule	Student scheduled courses	
	Teacher names	
Special Indicator	English language learner information	
	Low income status	
	Medical alerts /health data	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/ foster care)	
	Other indicator information- Please specify:	
Student Contact Information	Address	
	Email	
	Phone	
Student Identifiers	Local (School district) ID	

	number	
	State ID number	
	Provider/App assigned student ID number	
	Student app username	
	Student app passwords	
Student Name	First and/or Last	
Student In App Performance	Program/appli- cation performance (typing program-student types 60 wpm, reading program-student reads below grade level)	
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	
Student work	Student generated content; writing, pictures etc.	
	Other student	

	work data - Please specify:	
Transcript	Student course grades	
	Student course data	
	Student course grades/performance scores	
	Other transcript data -Please specify:	
Transportation	Student bus assignment	
	Student pick up and/or drop off location	
	Student bus card ID number	

	Other transportation data -Please specify:	
Other	Please list each additional data element used, stored or collected by your application	

No Student Data Collected at this time X .
 *Provider shall immediately notify LEA if this designation is no longer applicable.

OTHER: Use this box, if more space needed.

EXHIBIT “C”

DEFINITIONS

AB 1584, Buchanan: The statutory designation for what is now California Education Code § 49073.1, relating to pupil records.

De-Identifiable Information (DII): De-Identification refers to the process by which the Provider removes or obscures any Personally Identifiable Information (“PII”) from student records in a way that removes or minimizes the risk of disclosure of the identity of the individual and information about them.

Educational Records: Educational Records are official records, files and data directly related to a student and maintained by the school or local education agency, including but not limited to, records encompassing all the material kept in the student’s cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs. For purposes of this DPA, Educational Records are referred to as Student Data.

NIST: Draft National Institute of Standards and Technology (“NIST”) Special Publication Digital Authentication Guideline.

Operator: The term “Operator” means the operator of an Internet Website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used primarily for K–12 school purposes and was designed and marketed for K–12 school purposes. For the purpose of the Service Agreement, the term “Operator” is replaced by the term “Provider.” This term shall encompass the term “Third Party,” as it is found in applicable state statutes.

Personally Identifiable Information (PII): The terms “Personally Identifiable Information” or “PII” shall include, but are not limited to, student data, metadata, and user or pupil-generated content obtained by reason of the use of Provider’s software, website, service, or app, including mobile apps, whether gathered by Provider or provided by LEA or its users, students, or students’ parents/guardians. PII includes Indirect Identifiers, which is any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty. For purposes of this DPA, Personally Identifiable Information shall include the categories of information listed in the definition of Student Data.

Provider: For purposes of the Service Agreement, the term “Provider” means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of pupil records. Within the DPA the term “Provider” includes the term “Third Party” and the term “Operator” as used in applicable state statutes.

Pupil Generated Content: The term “pupil-generated content” means materials or content created by a pupil during and for the purpose of education including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of pupil content.

Pupil Records: Means both of the following: (1) Any information that directly relates to a pupil that is maintained by LEA and (2) any information acquired directly from the pupil through the use of instructional software or applications assigned to the pupil by a teacher or other LEA employee. For the purposes of this Agreement, Pupil Records shall be the same as Educational Records, Student Personal Information and Covered Information, all of which are deemed Student Data for the purposes of this Agreement.

Service Agreement: Refers to the Contract or Purchase Order to which this DPA supplements and modifies.

School Official: For the purposes of this Agreement and pursuant to 34 CFR 99.31 (B), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of education records; and (3) Is subject to 34 CFR 99.33(a) governing the use and re-disclosure of personally identifiable information from student records.

SOPIPA: Once passed, the requirements of SOPIPA were added to Chapter 22.2 (commencing with Section 22584) to Division 8 of the Business and Professions Code relating to privacy.

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, home address, telephone number, email address, or other information allowing online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information text messages, documents, student identifies, search activity, photos, voice recordings or geolocation information. Student Data shall constitute Pupil Records for the purposes of this Agreement, and for the purposes of California and federal laws and regulations. Student Data as specified in Exhibit "B" is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services.

SDPC (The Student Data Privacy Consortium): Refers to the national collaborative of schools, districts, regional, territories and state agencies, policy makers, trade organizations and marketplace providers addressing real-world, adaptable, and implementable solutions to growing data privacy concerns.

Student Personal Information: "Student Personal Information" means information collected through a school service that personally identifies an individual student or other information collected and maintained about an individual student that is linked to information that identifies an individual student, as identified by Washington Compact Provision 28A.604.010. For purposes of this DPA, Student Personal Information is referred to as Student Data.

Subscribing LEA: An LEA that was not party to the original Services Agreement and who accepts the Provider's General Offer of Privacy Terms.

Subprocessor: For the purposes of this Agreement, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its software, and who has access to PII.

Targeted Advertising: Targeted advertising means presenting an advertisement to a student where the selection of the advertisement is based on student information, student records or student generated content or inferred over time from the usage of the Provider's website, online service or mobile application by such student or the retention of such student's online activities or requests over time.

Third Party: The term "Third Party" means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of pupil records. However, for the purpose of this Agreement, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF DATA

San Joaquin County Office of Education directs Early Quality Systems-Hubbe Inc. to
dispose of data obtained by Provider pursuant to the terms of the Service Agreement
between LEA and Provider. The terms of the Disposition are set forth below:

<u>Extent of Disposition</u> Disposition shall be:	<input type="checkbox"/> Partial. The categories of data to be disposed of are as follows: <input type="checkbox"/> Complete. Disposition extends to all categories of data.
<u>Nature of Disposition</u> Disposition shall be by:	<input type="checkbox"/> Destruction or deletion of data. <input type="checkbox"/> Transfer of data. The data shall be transferred as set forth in an attachment to this Directive. Following confirmation from LEA that data was successfully transferred, Provider shall destroy or delete all applicable data.
<u>Timing of Disposition</u> Data shall be disposed of by the following date:	<input type="checkbox"/> As soon as commercially practicable <input type="checkbox"/> By (Insert Date) _____

Authorized Representative of LEA

Date

Verification of Disposition of Data
by Authorized Representative of Provider

Date

EXHIBIT "E"

GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and San Joaquin County Office and which is dated 05-21-2021 to any other LEA ("Subscribing LEA") who accepts this General Offer through its signature below. This General Offer shall extend only to privacy protections and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the other LEA may also agree to change the data provided by LEA to the Provider in Exhibit "B" to suit the unique needs of the LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statutes; (2) a material change in the services and products subject listed in the Originating Service Agreement; or three (3) years after the date of Provider's signature to this Form. Provider shall notify CETPA in the event of any withdrawal so that this information may be transmitted to the Alliance's users.

Provider: Early Quality Systems-Hubbe Inc.

BY:  _____

Date: 6/9/2021

Printed Name: Claire Crandall

Title/Position: Director

2. Subscribing LEA

A Subscribing LEA, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA.

Subscribing LEA:

BY: _____

Date: _____

Printed Name: _____

Title/Position: _____

TO ACCEPT THE GENERAL OFFER, THE SUBSCRIBING LEA MUST DELIVER THIS SIGNED EXHIBIT TO THE PERSON AND EMAIL ADDRESS LISTED BELOW

Name: _____

Title: _____

Email Address: _____

EXHIBIT “F” DATA SECURITY REQUIREMENTS

[INSERT ADDITIONAL DATA SECURITY REQUIREMENTS HERE]

All Pupil Records housed in QRIS Hubbe California are and shall remain the sole property of the LEA or preschool agency under contract with Hubbe Inc.

QRIS Hubbe California is an adult-managed data system for infant, toddler and preschool programs. Unlike K-12 Student Information Systems, there are no features or modules that are designed for student/child access/use due to the very young age of the children in early childhood education programs.

QRIS Hubbe is an adult-managed data Assessment for infant, toddler and preschool programs. Unlike K-12 Student Information Systems, there are no features or modules that are designed for student/child use due to the age of the children in early childhood education programs.

QRIS Hubbe California hosts a secure/FERPA-Compliant parent portal where parents can access information about their family, themselves and their children. The parent portal serves as the method for parents to review data, correct erroneous information, and communicate with the agency to update data and records as needed as determined by The LEA/Preschool Agency ' s policies and procedures. QRIS Hubbe California was designed for early childhood education providers serving children ages 0-5. The system does not have components for use by young children ages 0-5. As such, it is an adult-only system.

In order to maintain the security and confidentiality of all Pupil Records, the following security and confidentiality policies are enforced by the Chief Information Security Officer (CISO):

Hubbe Inc. will obtain a criminal background check of each applicant prior to the commencement of the applicant ' s employment. Hubbe Inc. utilizes Goodhire to conduct background checks. A report of the background check will be stored in each employee ' s file.

All offers of employment shall be subject to satisfactory criminal report

- All offers of employment shall be subject to satisfactory criminal report investigations.
- All new employees and independent contractors who perform services in the production systems and have access to customer information will participate in the *Hubbe Inc.* security and confidentiality training. Each person shall sign and acknowledge his or her agreement to abide by the *Hubbe Inc.* security and confidentiality policies. Training will recur at least once each year, or sooner, as determined by *Hubbe Inc.* management and as required by changes to the policies. Such training program shall include, at a minimum, basic steps to maintain the security, confidentiality and integrity of customer information, such as:
 - Identifying for employees and independent contractors the types of customer information subject to protection under the security and confidentiality policies.
 - Using password-activated computer and software systems and applications and automatic log-off function that terminates access after a short period of inactivity.
 - Using strong passwords (at least eight characters long and alpha-numeric).
 - Changing passwords periodically and maintaining the security of passwords.
 - Sending electronic information over secure channels only.
 - Appropriately disposing of paper and electronic records.
- All employees and independent contractors will be permitted to access customer information only when "needed to de-bug software and/or support client's needs as requested. Access to client data will be determined individually by *Hubbe Inc.* management.
- Personnel shall not be permitted to access, use or reproduce customer information, whether electronic or non-electronic, for their own use or for any use not authorized by *Hubbe Inc.* management.
- All persons who fail to comply with the *Hubbe Inc.* security and confidentiality policies shall be subject to disciplinary measures, up to and including termination of employment for employees or contract termination for independent contractors that perform services with *Hubbe Inc.*

8. In the event of an unauthorized disclosure of a pupil's records, Service Provider shall Report to an affected parent, legal guardian, or eligible pupil pursuant to the following Procedure:

- Validate the data breach. Do not assume that every identified incident is actually a breach of PII. Examine the initial information and available logs to confirm that a breach has occurred. If possible, identify the type of information disclosed and estimate the method of disclosure (internal/external disclosure, malicious attack, or accidental).
- Begin breach response documentation and reporting process. Coordinate the flow of information to Client
- Include representatives from *Hubbe Inc.* And Client management, information technology, legal, public affairs media relations, risk management, finance, and audit departments (and possibly HR, for internal incidents) in the incident response team.
- Immediately determine the status of the breach (on-going, active, or post breach).
- If the breach is active or on-going, take action to prevent further data loss by securing and blocking unauthorized access to Systems/data and preserve evidence for investigation.
- Document all mitigation efforts for later analyQRIS.

- Advise staff who are informed of the breach to keep breach details in confidence until notified otherwise.
- If criminal activity is suspected, notify law enforcement and follow any applicable federal, State, or local legal requirements relating to the notification of law enforcement. (The decision to involve outside entities, including law enforcement, should generally be made in consultation with executive leadership and legal counsel.)
- Identify all affected data, machines, and devices.
- Conduct interviews with key personnel and document facts (if criminal activity is suspected, coordinate these interviews with law enforcement).
- When possible, preserve evidence (backups, images, hardware, etc.) for later forensic examination.
- Locate, obtain, and preserve (when possible) all written and electronic logs and records applicable to the breach for examination.
- Reach out to data owners as soon as possible to notify them about the breach.
- Foster a cooperative relationship between the incident response team and data owners.
- Work collaboratively with data owners to secure sensitive data, mitigate the damage that may arise from the breach, and determine the root cause(s) of the breach to devise mitigating strategies and prevent future occurrences.

9. Service Provider shall not use any information in a pupil record for any purpose other than those required or specifically permitted by the Technology Services Agreement.

10. Service Provider certifies that a pupil's records shall not be retained or available to the Service Provider upon completion of the terms of the Technology Services Agreement, 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:

- *Hubbe Inc.* provides extensive data export capabilities allowing the export of all *QRIS Hubbe* data to its customer at any time. This process may be executed at the end of contract period or at any time desired.
- Customer should first ensure that browser downloads of *QRIS Hubbe* data go to a secure download environment
all *QRIS Hubbe* downloads are done via SSL browser should be set to download on a secure/encrypted drive
- Download all data by following these steps
 - * In *QRIS Hubbe*, Log on as admin user. From main menu go to "Data Tools" then the "Export Data."
 - * for each data item select item type (radio button) and then select export each export file will be downloaded as an excel file

11. LEA agrees to work with Service Provider to ensure compliance with FERPA and the Parties will ensure compliance through the following procedure:

Hubbe Inc. FERPA Policy

The Family Educational Rights and Privacy Act, known as FERPA, protects the privacy interests of students in their education records. It controls the disclosure of a student's personally identifiable information from education records without the consent of the parent or eligible student. As part of the *Hubbe Inc. Data Systems*, agencies staff and parents enter personally identifiable information about their infant, toddler, and preschool students/children into the *QRIS Hubbe California Systems, QRISHubbe.com*, in order to operate their program and report data to program funders. *QRIS Hubbe California* supplies capabilities for the agencies and parents to use the personally identifiable information in the context of a Student Information and Program Management System. *Hubbe Inc.* has no direct use of the personally identifiable information. *Hubbe Inc.* agrees to only use the personally identifiable student information supplied by the agencies and funder to provide training on the data system and/or to support their data system needs and to return or delete the personally identifiable information when the funder is no longer under contract with *Hubbe Inc.* In this way, the data owner retains control over its PII data as required under FERPA. *Hubbe Inc.* does not data-mine or commercialize information held for LEAs/Preschool Agencies and it does not collect any information directly from students or their parents for its use.

Hubbe hosts a secure, FERPA-Compliant web-based data system using Amazon Web Service (AWS) following the guidelines as set forth in FERPA Compliance on AWS Family Educational Rights and Privacy Act of 1974 (FERPA) whitepaper available at: https://d0.awsstatic.com/whitepapers/compliance/AWS_FERPA_Whitepaper.pdf
Additional information on Amazon AWS policies can be accessed at: <https://aws.amazon.com>.

Under the direction of the CISO, the *Hubbe Inc.* staff follow the best practices recommended by Amazon AWS by implementing the following FERPA compliant environment:

- **Compute** - *Hubbe* uses AWS cloud to store, process and transmit PII, and leverage encryption at layers to safeguard the data at rest and in transit additional details below. Ensure the systems are properly hardened and monitored for compliance.
- **Storage** - *Hubbe* configures data storage for least privilege and data is not world accessible, except by managed exceptions
- **Database** - *Hubbe* uses Microsoft SQL Server which provides SQL Server Transparent Data Encryption (TDE) and Cell Level Encryption (CLE) server-side facilities that encrypt the entire SQL Server database at rest, or selected columns as needed. This encryption uses Advanced Encryption Standard (AES) 256, a secure symmetric-key encryption standard using 256-bit encryption keys.
- **Networking and content delivery** – *Hubbe* provides a logically isolated network for processing, transmitting or storing PII.
- **Security, identity, and compliance** – *Hubbe* uses Amazon GuardDuty to detect misconfigurations, provide threat intelligence such as instances communicating with known bad actors as well as alerting and automating to remediate these issues.

Under the direction of the CISO, the *Hubbe Inc.* staff follow the best practices recommended by Amazon AWS by following FERPA compliant information management:

- **Auditing** – *Hubbe* auditing capabilities are in place to allow security analysts to examine detailed activity logs and reports.

- **Data destruction** – *Hubbe* uses DoD-compliant drive and file wipe/erasure software to remove PII data.
- **Backup and disaster recovery** – *Hubbe* creates periodic (every two hours) database backups and creates point-in-time snapshots of volumes daily.
- **Security** - All *Hubbe* Inc. Data Systems utilized by clients use Secure Sockets Layer (SSL) certifications, so that the security of such information is protected in transit. Such secure transmissions shall be automatic. Attempts to access *Hubbe* Inc. Data Systems without SSL will automatically be rerouted to a SSL connection.
- **Authentication and authorization** - In the AWS environment, *Hubbe* uses IAM to manage access keys, security credentials, permission levels, authentication and authorization of our AWS accounts. The AWS account is protected by both password and Multi-Factor Authentication (<https://aws.amazon.com/iam/details/mfa/>)
- **Threat detection** - *Hubbe* uses Amazon GuardDuty's machine learning capability to uncover malicious user activity within AWS accounts. Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect accounts, workloads, and data stored in AWS.
- **Security logs** - *Hubbe* uses Amazon CloudWatch to detect anomalous behavior in our environments, set alarms, analyze logs and metrics, take automated actions, and troubleshoot issues. Cloudwatch allows us to improve operational performance and resource optimization.