

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

School District/Local Education Agency:

San Marcos Unified School District

AND

Provider:

DataHouse Consulting, Inc.

(Hereinafter referred to as "DataHouse")

Date:

October 4, 2020

This California Student Data Privacy Agreement (“DPA”) is entered into by and between the
San Marcos Unified School District

(hereinafter referred to as “LEA”) and DataHouse Consulting, Inc
(hereinafter referred to as “Provider”) on October 4, 2020 . 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 October 2, 2020 (“Service Agreement”); and

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:

See Exhibit "A"

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, PPRA, 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, PPRA, 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: Mark Schiel
Title: Asst. Superintendent, Business Svcs.

Contact Information:
San Marcos Unified School District
255 Pico Ave, Ste 250, San Marcos, CA 92069
mark.schiel@smusd.org

The designated representative for the Provider for this Agreement is:

Name: Hong Phan
Title: President

Contact Information:
DataHouse Consulting, Inc.
1585 Kapiolani Blvd, Suite 1800
Honolulu, HI 96814

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: Hong Phan
Title: President

Contact Information:
DataHouse Consulting, Inc.
1585 Kapiolani Blvd, Suite 1800
Honolulu, HI 96814

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: DataHouse Consulting, Inc.

BY:  Date: 10/04/2020

Printed Name: Hong Phan Title/Position: President

Local Education Agency: San Marcos Unified School District

BY:  Date: 10/17/20

Printed Name: Mark Schiel Title/Position: Asst. Superintendent, Business Svcs.

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]

I. LumiSight Campus Platform Overview

The impacts of COVID-19 have challenged many of California's families and schools, but there is still hope for a brighter future.

While individuals adjust to the ongoing changes, education leaders can help lead our community to better health by proactively monitoring their school environments for their students, faculty, and staff. With the right platform and processes, organizations like San Marcos Unified School District (SMUSD) can help steer our K-12 community's fate in a promising direction.

To help improve administration processes, DataHouse. has developed the LumiSight Campus Platform so that students, faculty, staff, and visitors can precheck their health status and receive guidance on whether they can report to campus. The platform aligns with CDC Guidance for Community, Work, and School to prevent and reduce transmission among the students, faculty, staff, and visitors, promoting accountability within the SMUSD community.

The LumiSight Campus Platform includes the following:

- **Web and mobile application** for users to submit daily check-ins
- **Notifications** for daily reminders and to send customized messages to specific groups
- **Geofencing perimeters** for additional layers of protection
- **Administration dashboard** for administrators to update configurations of the application

The platform is easy-to-use and enables users to complete all forms and information effortlessly. With the standard and optional features, schools can strengthen their COVID-19 response strategies and proactively respond to potential risks within the community.

The following sections continue with LumiSight Campus and provide an overview of the web, mobile, and administration applications.

A. Web and Mobile Applications

LumiSight is a screening and surveillance platform that makes it easy for individuals to provide a daily check-in of their health status before leaving their home or going to school. Users have quick access to the applications from their desktop, laptop, phone, or tablet, and the apps are easy to use every day.

Users simply:

1. Log in and consent
2. Confirm their information
3. Select their settings
4. Check in
5. View their results



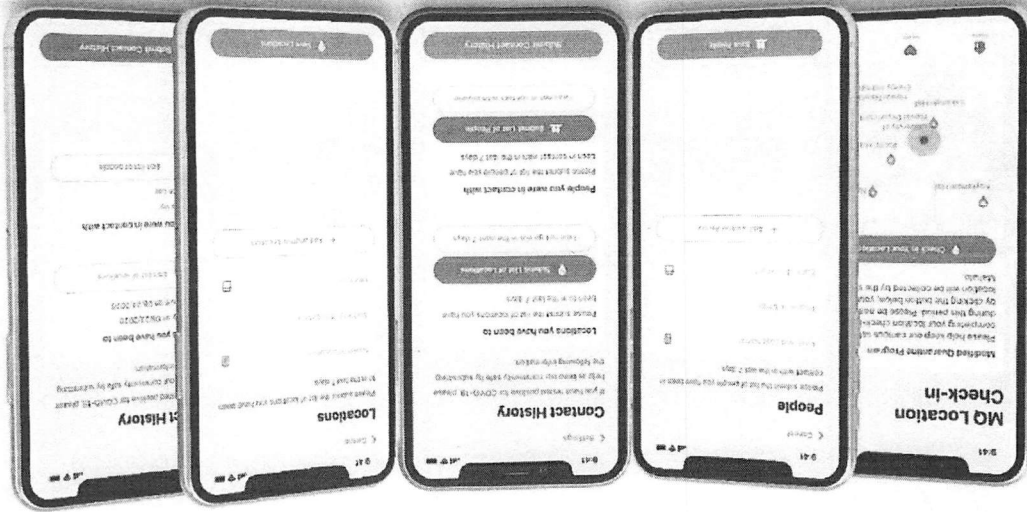
With the web application users can create an account, complete an initial assessment, then perform daily check-ins and receive results immediately. Users have easy access to Lumisight Campus from their desktop, laptop, phone, or tablet. The following shows the user journey through the application. Note that the following screens are examples only and are subject to change.

Visitors can also create accounts and submit a check-in before they come on site. Visitors can be one-time guests or recurring, infrequent visitors such as vendors. With the visitor feature, SMUSD can hold such individuals accountable and enforce organizational policies while safeguarding information privacy.

Lumisight Campus also offers features to expand organizational capabilities such as:

- **Contact tracing** for person and location history reporting
- **Quarantine monitoring** of designated users to check in their location
- **Multi-lingual capability** (e.g., Spanish) for users to select

As an example, the Contact Tracing feature enables person and location history tracking and reporting. Users can enter the names of people with whom they have been in contact and the locations where they visited. Then, Lumisight administrators receive information on the admin dashboard to perform contact tracing activities or prevent a potential breakout.



B. Administration Dashboard

LumiSight Campus Platform comes with a responsive web-based administration dashboard to monitor and track data.

- View and manage check-ins per day
 - Push notifications to users
 - View detailed analytics
- App usage
Users advised to NOT report to the office
Proactive communication

The following image is a sample dashboard where administrators can quickly view daily check-in statistics among the community.



The next images show more detailed check-in information for users.

Check-ins

All Students Faculty Visitors External

Monday, June 8, 2020

NAME	ID	EMAIL	STATUS	LOCATION
James Doe	123456	james.doe@lumisight.com	Check-in	Building A
John Doe	123457	john.doe@lumisight.com	Not Clear	Building A
John Doe	123458	john.doe@lumisight.com	Clear	Building A
John Doe	123459	john.doe@lumisight.com	---	Building A
John Doe	123460	john.doe@lumisight.com	Clear	Building A
John Doe	123461	john.doe@lumisight.com	Not Checked	Building A
John Doe	123462	john.doe@lumisight.com	---	Building A
John Doe	123463	john.doe@lumisight.com	Clear	Building A
John Doe	123464	john.doe@lumisight.com	Not Clear	Building A
John Doe	123465	john.doe@lumisight.com	---	Building A
John Doe	123466	john.doe@lumisight.com	---	Building A
John Doe	123467	john.doe@lumisight.com	---	Building A
John Doe	123468	john.doe@lumisight.com	---	Building A
John Doe	123469	john.doe@lumisight.com	---	Building A

10 Results per page

Manage Users

All Students Faculty Visitors

Monday, June 8, 2020

NAME	ID	EMAIL	PHONE	STATUS
James Doe	123456	james.doe@lumisight.com	555-555-5555	Active
John Doe	123457	john.doe@lumisight.com	555-555-5556	Inactive
John Doe	123458	john.doe@lumisight.com	555-555-5557	Terminated
John Doe	123459	john.doe@lumisight.com	555-555-5558	Active
John Doe	123460	john.doe@lumisight.com	555-555-5559	Active
John Doe	123461	john.doe@lumisight.com	555-555-5560	Active
John Doe	123462	john.doe@lumisight.com	555-555-5561	Active
John Doe	123463	john.doe@lumisight.com	555-555-5562	Active
John Doe	123464	john.doe@lumisight.com	555-555-5563	Active
John Doe	123465	john.doe@lumisight.com	555-555-5564	Active
John Doe	123466	john.doe@lumisight.com	555-555-5565	Active
John Doe	123467	john.doe@lumisight.com	555-555-5566	Active
John Doe	123468	john.doe@lumisight.com	555-555-5567	Active
John Doe	123469	john.doe@lumisight.com	555-555-5568	Active
John Doe	123470	john.doe@lumisight.com	555-555-5569	Active

10 Results per page

User Permissions

Role	Category	Item	Value
Web Admin	Symptom	View Symptom	True
Web Admin	Symptom	Create Symptom	True
Web Admin	Symptom	Update Symptom	True
Web Admin	Symptom	Delete Symptom	True
Web Admin	Result	View Result	True
Web Admin	Result	Create Result	True
Web Admin	Result	Update Result	True
Web Admin	Result	Delete Result	True
User	Permissions	View Permissions	True
User	Permissions	Create Permission	True
User	Permissions	Update Permission	True
User	Permissions	Delete Permission	True
Admin	Notifications	View Notification	True
Admin	Notifications	Create Notification	True
Admin	Notifications	Update Notification	True
Admin	Notifications	Delete Notification	True

II. LumiSight Campus Platform Implementation

DataHouse will provide the following for SMUSD:

1. The LumiSight Campus Platform, which is a cloud-based Software as a Service (SaaS) solution that includes the following:
 - a. Web and mobile applications
 - b. Notifications
 - c. Geofencing
 - d. Contact tracing
 - e. Quarantine monitoring
 - f. Multi-lingual option (e.g., Spanish)
 - g. Administration dashboard
2. LumiSight Campus Platform implementation services, including:
 - a. Platform setup
 - b. User Quick Guide
 - c. One online user orientation session
 - d. One online administrator session
 - e. Post-deployment support for up to two administrators

III. Configuration Process

DataHouse uses a simple process to configure the LumiSight Campus Platform.



The next sections summarize each stage in the process.

A. Plan

During the Plan stage, DataHouse works closely with a designated SMUSD stakeholder to plan the configuration, including an agreed-upon start date and go-live plan. Planning is estimated to take no more than one business day.

B. Configure

When planning is complete, DataHouse will configure and test the platform to ensure its functionality.

C. Deploy

Once the configuration is complete, DataHouse will deploy the platform. We will follow an agreed-upon go-live schedule.

Additionally, DataHouse is committed to maximizing SMUSD's technology investment by providing thorough training and knowledge transfer throughout the process. Since training is critical to the overall success of the implementation, and usability is the key to user success, we provide train-the-trainer, LumiSight administration dashboard training for administrators, and user guides.

As part of DataHouse's strategic product success planning, our knowledge transfer approach prepares SMUSD for the continued operation and support of the system. Knowledge transfer activities occur throughout the entire process, including planning, meetings, go-live, and post-deployment.

After go-live, DataHouse will provide Tier 2 support for authorized named users or up to two administrators through the LumiSight Support Portal. The process for submitting and managing cases is described as follows:

Support	Role	Description
Tier 1 Support	SMUSD Tier 1 Support	<p>SMUSD Tier 1 Support will be the primary and first point of contact. They will make the initial attempt to diagnose and resolve the issue. Once the case has been resolved, Tier 1 Support will close the case.</p> <p>If the Tier 1 Support is unable to resolve the issue, they can escalate to DataHouse Tier 2 Support for resolution. Tier 1 Support must create a case and document the issue in the LumiSight Support Portal at https://lumisight-support.DataHouse.com</p>
Tier 2 Support	DataHouse Tier 2 LumiSight Platform Support Consultant	<p>DataHouse Tier 2 Support receive cases from the SMUSD Tier 1 Support via the LumiSight Support Portal. If the issue is platform related, they will determine if any changes or updates are necessary to resolve the issue.</p> <p>Otherwise, the case will be escalated to the product team for further troubleshooting and resolution.</p>

IV. Assumptions

The following assumptions have been factored into the timeline estimates provided in this proposal. Any deviation from these assumptions may alter the approach and estimates.

- DataHouse is providing one (1) environment and one (1) database instance of LumiSight Campus.
- LumiSight branding will be used.
- All users will have an email address.
- DataHouse is not responsible for delays or additional scope that results from other initiatives the client may have in progress.
- SMUSD will provide qualified and knowledgeable members to the project team at the staffing levels necessary and according to the timeline, with the business and technical skills required.

- SMUSD will assign one (1) person to serve as DataHouse’s primary point of contact during the project. This person will have signature and decision authority, manage all internal communications, and assist DataHouse with logistics.
- SMUSD will respond to inquiries within 24 hours.
- SMUSD will be scheduled and held to an agreed-upon timeline to ensure consistency of resources for the project.
- Additional services not included in this proposal will go through a change request process.
- LumiSight Campus Platform mobile application is subject to approval by Apple and Google.
- LumiSight Campus mobile application supports the following:
 - Android and iOS mobile phones
 - Android Operating System 7.0 and above
 - iOS Operating System
 - OS Operating System 10.0 and above
- Product maintenance releases may be applied as appropriate.
- Geofencing is limited to twenty (20) geocodes.
- Automatic annual payments will apply unless DataHouse receives a cancellation notice within 30 days of the renewal date.

V. LumiSight Campus Platform License Agreement

DataHouse Consulting, Inc. (“Licensor”) owns and operates the LumiSight Campus Platform (“Software”) and hereby grants to SMUSD (“Licensee”) a non-exclusive, non-transferable License to use the Software in accordance with the Agreement.

LICENSEE’S OBLIGATIONS

Licensee may permit its employees and agents to use the Software for the purposes described herein, provided that Licensee takes all necessary steps to ensure that all employees and agents using the Software do not disclose the contents of it to any third person or use it in any way other than in accordance with the terms of this Agreement.

Licensee shall not distribute, sell license or sub-license, let, trade or expose for sale the Software to any third party.

Licensee shall not assign any rights of this Agreement without the prior written consent of Licensor.

INTELLECTUAL PROPRIETARY RIGHTS

Licensee acknowledges and agrees that the Software and all content is protected by copyrights, trademarks, service marks and/or other proprietary protections to which Licensor owns and retains all rights, title and interests.

Licensee shall not reverse engineer, modify, distribute, copy, reproduce, transmit, publicly display or create derivative works of the Software or its content and materials.

LIMITATION OF LIABILITY

Licensee agrees that Licensor shall not be responsible or liable to Licensee or any third party for any information sent, received or relied upon through the Software. Licensee agrees to release Licensor from any and all claims arising out of or related to the use of the Software.

Licensor shall not be liable for any claim whatsoever arising out of or related to the Software for: a) any matter beyond its reasonable control, b) loss or inaccuracy of data, loss or interruption of use, goods or services, c) reliance on inaccurate or erroneous data or d) indirect, punitive, incidental, reliance, special, exemplary or consequential damages.

INDEMNIFICATION

Licensee agrees to: a) hold harmless and defend Licensor and its employees, agents, contractors, officers, directors and representatives against any action by a third party that arises out of any transaction with the Software and b) indemnify Licensor for settlement amounts or damages, liabilities, costs and expenses including reasonable attorneys' fees.

DISCLAIMER OF WARRANTIES

Licensor does not warrant the accuracy, timeliness or quality of the data that it collects from third parties or that the Software will function in any environment error-free, uninterrupted or free from viruses or harmful components.

CHOICE OF LAW AND FORUM

Licensee agrees that any claim or cause of action arising out of or related to the Software must commence within one (1) year after the date of occurrence.

This Agreement shall be governed by and construed in accordance with the laws of the State of Hawaii, in the county of Honolulu. Licensee expressly agrees that the exclusive jurisdiction for any claim or action arising out of or relating to the Agreement or use of the Software shall be in the State of Hawaii.

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	
Assessment	Standardized test scores	
	Observation data	
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications that are captured (emails, blog entries)	

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	X
	Student grade level	X
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information-Please specify:	
Parent/Guardian Contact Information	Address	
	Email	X
	Phone	X

Parent/ Guardian ID	Parent ID number (created to link parents to students)	X
Parent/ Guardian Name	First and/or Last	X
Schedule	Student scheduled courses	
	Teacher names	X
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	x
	Phone	x
Student Identifiers	Local (School district) ID	X

	number	
	State ID number	
	Provider/App assigned student ID number	X
	Student app username	X
	Student app passwords	X
Student Name	First and/or Last	X
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	X
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	school location, Date and time of check-in, Check-in result

No Student Data Collected at this time_____.
 *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.

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 Marcos Unified School District

directs

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:

<p><u>Extent of Disposition</u></p> <p>Disposition shall be:</p>	<p>___ Partial. The categories of data to be disposed of are as follows:</p> <p>___ Complete. Disposition extends to all categories of data.</p>
<p><u>Nature of Disposition</u></p> <p>Disposition shall be by:</p>	<p>___ Destruction or deletion of data.</p> <p>___ 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.</p>
<p><u>Timing of Disposition</u></p> <p>Data shall be disposed of by the following date:</p>	<p>___ As soon as commercially practicable</p> <p>___ By (Insert Date) _____</p>

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 Marcos Unified**

and which is dated **October 2, 2020** to any other LEA ("Subscribing LEA") who accepts this

General Offer though 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: **DataHouse Consulting, Inc**

BY: 
Printed Name: Hong Phan

Date: 10/04/2020
Title/Position: President

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: _____
Printed Name: _____

Date: _____
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]

Not Applicable