

Vendor Statement of Compliance Data Privacy and Protection

This agreement is entered into between the Roseville City School District ("LEA" or "District") and Luminous Minds Inc ("Service Provider") on 01/27/2025 ("Effective Date").

WHEREAS, the LEA and the Service Provider entered into an agreement for Educational Technology services;

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

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

NOW, THEREFORE, the Parties agree as follows:

Section I: General - All Data

1. **PASSWORD SECURITY.** All passwords are considered secure. Vendors may not disseminate any passwords unless specifically directed by Educational or Technology Services management. Vendors will not provide information concerning Admin accounts (ROOT Admin, container Admin, local NT administrator or Domain administrator) or their equivalent to any persons. District personnel ONLY will disseminate this information. Vendors will never create "back door" or "generic" user accounts on any systems unless specifically directed to do so by LEA management.

Agree: Yes No

2. **SYSTEM SECURITY.** Unauthorized access to or modification of District systems including file servers, routers, switches, NDS and Internet services is prohibited. Any attempt to bypass or subvert any District security system, both hardware, and software is prohibited.

Agree: Yes No

3. **PRIVACY.** The vendor will adhere to all provisions of the Federal Family Educational Rights and Privacy Act (FERPA, 20 U.S.C. 123g), California Education Code and district policies regarding the protection and confidentiality of data. At all times, the vendor will consider all data collected in the course of their duties to be protected and confidential. Release of this data can only be authorized by Technology & Information Services management and state and federal law.

Agree: Yes No

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

Section I: General - All Data (Continued)

4. **REUSE:** Vendors shall not copy, duplicate, sell, repackage or use for demonstration purposes any Roseville City School District data without the prior, written consent of Educational or Technology Services management.

Agree: Yes No

5. **TRANSPORT:** Vendor must provide a secure channel (S/FTP, HTTPS, SSH, VPN, etc) for the District to "push" data to the vendor and to extract data as required. Vendors will not have direct access to District systems and will not "pull" data at any time.

Agree: Yes No

6. **EXTERNAL SECURITY:** Vendor must attach to this document reasonable evidence that their system is secure from external hacking and attacks. Devices such as firewalls and technologies such as NAT are the minimum requirements. Active IDS or similar technology is preferred.

Agree: Yes No

7. **INTERNAL SECURITY:** Vendors must attach to this document reasonable evidence that their system is secure from internal hacking and attacks. Describe the interactions vendor personal (or their representatives) will have directly with District data. How is uploaded data from the District handled and processed? Who has access to this data? What happens to the data after the upload is complete? What security safeguards are in place to protected unauthorized access to District data? How are backup performed and who has access to and custody of the backup media? How long are backup maintained; what happens to the District data once the backup is "expired"? If any data is printed, what happens to these hard copy records?

Agree: Yes No

8. **DISTRICT ACCESS:** Vendor must provide a secure means (see Item 5 above) for the District to extract ALL data from the vendor system. This can either be an online extraction tool or a vendor-provided extract as needed by the District (not to exceed quarterly). Describe the means and format of the data (delimited, Excel, MDB, SQL Dump).

Agree: Yes No

9. **TERMINATION:** Upon termination of this agreement as provided herein, the vendor will permanently delete all customer data from their system as allowed by state and federal law. Vendor may be required to certify the destruction of LEA data within 90 days of contract termination.

Agree: Yes No

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

Section II: AB1584 Compliance - Student Information Only

1. Vendor agrees that the Roseville City School District retains ownership and control of all student data.
Agree: Yes No
2. Vendor must attach to this document a description of how student-created content can be exported and/or transferred to a personal account.
Agree: Yes No
3. Vendor is prohibited from allowing third-parties access to student information beyond those purposes defined in the contract.
Agree: Yes No
4. Vendor must attach to this document a description of how parents, legal guardians and students can review and correct their personally identifiable information.
Agree: Yes No
5. Vendor will attach to this document evidence how student data is kept secure and confidential.
Agree: Yes No
6. Vendor will attach to this document a description of procedures for notifying affected parents, legal guardians or eligible students when there is an unauthorized disclosure of student records.
Agree: Yes No
7. Vendor certifies that student records will not be retained or available to a third party once the contract has expired or is canceled (See Page 2, Item 9).
Agree: Yes No
8. Vendor will attach to this document a description of how they and any third party affiliates comply with FERPA.
Agree: Yes No
9. Vendor and its agents or third parties are prohibited from using personally identifiable information from student records to target advertising to students
Agree: Yes No

Section III: SB 1177 SOPIPA Compliance - Student Information Only

1. Vendors cannot target advertising on their website or any other website using information acquired from students.
Agree: Yes No
2. Vendors cannot create a profile for a student except for school purposes as defined in the executed contract.
Agree: Yes No
3. Vendors cannot sell student information.
Agree: Yes No
4. Vendors cannot disclose student information unless for legal, regulatory, judicial, safety or operational improvement reasons.
Agree: Yes No
5. Vendors must attach to this document evidence of how student information is protected through reasonable security procedures and practices.
Agree: Yes No
6. Vendors must delete district-controlled student information when requested by the District.
Agree: Yes No
7. Vendors must disclose student information when required by law, for legitimate research purposes and for school purposes to educational agencies.
Agree: Yes No

As an authorized representative of my organization, I accept the conditions listed in this document.

Chandra Roughton

Print Name

Chandra Roughton Jan. 27, 2025
Signature, Date

Laura Assem

Print Name (Roseville City School District)

Laura Assem 2/5/2025
Signature, Date (Roseville City School District)

EXHIBITS

Section 1.6: External Security

Please see Exhibit A.

Section 1.7: Internal Security

Please see Exhibit A.

Section II.2: Exporting of Student-Created Content

NA

Section II.4: Review and Correcting Personally Identifiable Information (PII)

See LMI privacy agreement

EXHIBITS

Section II.5: Securing Student Data

Please see Exhibit A.

Section II.6: Disclosure Notification

See LMI data privacy agreement

Section II.8: Family Educational Rights and Privacy Act (FERPA) Compliance

See LMI data privacy agreement

Section III.5: How Student Data is Protected:

Please see Exhibit A.

Section 1.6 External Security:

Our platform is hosted in a Google datacenter through Siteground. You can find comprehensive details about the encryption methods we use at <https://cloud.google.com/docs/security/encryption/default-encryption#:~:text=All%20data%20that%20is%20stored,encryption%20consistently%20across%20Google%20Cloud> . Our platform is hosted by Google datacenter situated in Iowa, US. The datacenter is STAR certified. Please refer to details on this link <https://cloudsecurityalliance.org/star/registry/google> .

All firewalls and protections are in place to ensure the highest level of security.

Section 1.7 Internal Security:

By default, we encrypt all information using SSL/TLS Encryption.

All accounts are imported by the Luminous Minds team from a CSV spreadsheet or manual entry. The only data collected is teacher first name, teacher last name, and school email. Additionally, we are a certified app through Clever, adhering to SSO.

User activity gets logged internally, however, this is only for our troubleshooting process and is not shared nor visible in the school, teacher, or student dashboards.

Our software has the ability to set field-level security for read, read/write and no access. This is defined at the code-level; more specifically in the plugin responsible for managing schools, teachers, & students, where role-control, as well as the capabilities each role has, is critical for the good functioning of the project.

Our application does not share any information from user dashboards (school, teacher, or student data) with third parties. Only Luminous Minds team members with administrative privileges can access District data.

Our educational website does not transfer any data/reports. We offer a library of pre-recorded, guided video lessons that teachers can project and play to the whole class, or assign to students individually. Students do not interact with the software, they simply watch educational reading lessons. Some lessons have corresponding worksheets/activities, but these are completed on paper during or following the lesson. We can send user activity reports, but there are no 'assignments' or 'assessments' or student data that would be received nor transferred.

Backups are performed weekly, including full security reports. Backups are generated at the Iowa server, encrypted, and then transmitted to the datacenter machines in Virginia. In the event of an emergency, our hosting company has the capability to swiftly restore all data to a previous state.

Additionally, all communication between servers is securely encrypted using TLS 1.3. Backups are accessible by the Head of Maintenance. Backups are maintained for the longevity of the District/school contract. Upon completion or end of a contract term, data is removed within 45 days unless the District requests that we securely store it for longer. No data is printed.

Section 1.8 District Access:

We can provide a secure transfer of all data from our system through a vendor provided extract in the form of a secure CSV delimited file.

Section II.2 Exporting of Student-Created Content:

NA - no student created content is available on our platform.

Section II.4 Reviewing and Correcting Personally Identifiable Information (PII):

For teacher access, the only PII collected is: teacher first name, teacher last name, and school email. Our admin team and website customer support can easily update an email address, name change, or other change through our 'School Site Access' platform. For students, we collect student first name, student last name, and a student ID number. This number can be provided by the school and/or randomly generated from our system. Our admin team will correct any erroneous information in reference to a student's PII within 24-72 hours. Teachers have access to 'manage' their students, in which they are able to 'add' or 'remove' students. Removal of a student permanently removes them from the system. Teachers are also able to update and/or change student passwords.

Section II.5 Securing Student Data:

Please see answer Section 1.7.

Section II.6 Disclosure Notification:

Please see LMI Privacy Agreement.

Section II.8 Family Educational Rights and Privacy Act (FERPA) Compliance:

Please see LMI Privacy Agreement.

Section III.5 How Student Data is Protected:

Please see answer Section 1.7.

DATA PRIVACY AGREEMENT

This Data Privacy Agreement (“**DPA**”) is entered into by and between [Roseville City School District](#) (“**LEA**”) and Luminous Minds, Inc. (“**Provider**”). LEA and Provider are each referred to herein as a “**Party**” and collectively, as the “**Parties**.” The Parties agree to the terms as stated herein.

RECITALS

WHEREAS, Provider provides certain educational products and services to customers, including schools and school districts; and

WHEREAS, Provider may receive or create, and the LEA may provide documents or data (“**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 Data also is subject to California state student privacy laws, including California Education Code Section 49073.1 and the Student Online Personal Information Protection Act (“**SOPIPA**”) (California Business and Professions Code section 22584); and

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

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

ARTICLE 1 PURPOSE AND SCOPE

1.1 **Purpose of DPA.** The purpose of this DPA is to describe the duties and responsibilities of Provider to protect the Data transmitted to Provider from LEA, including compliance with all applicable statutes and other applicable California laws, all as may be amended from time to time.

1.2 **Student Data to Be Provided.** LEA shall provide the Data necessary, which may include Student Data, for Provider to provide the requested products and services.

1.3 **DPA Definitions.** The definition of terms used in this DPA are found in Exhibit “A”.

ARTICLE 2 DATA OWNERSHIP AND AUTHORIZED ACCESS

2.1 **Data Ownership.** All Data transmitted to, or collected by Provider is, and will

continue to be, the property of and under the control of the LEA. Provider further acknowledges and agrees that all copies of such Data transmitted to 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 Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Data shall remain the exclusive property of the LEA. For the purposes of FERPA if applicable, Provider shall be considered a School Official, under the control and direction of the LEA as it pertains to the use of Student Data. Provider may transfer pupil-generated content to a separate account, according to the procedures set forth below.

2.2 **Parent Access.** If Provider collects or receives Student Data, 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 Provider to view or correct as necessary. In the event that a parent of a pupil or other individual contacts Provider to review any of the Student Data accessed pursuant to the Services, Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.

2.3 **Separate Account.** If pupil generated content is stored or maintained by Provider, Provider shall, at the request of the LEA, transfer said pupil generated content to a separate student account upon termination of LEA's use of Provider's products; provided, however, such transfer shall only apply to pupil generated content that is severable from the Student Data.

2.4 **Third Party Request.** Should a third party, including law enforcement and government entities, contact Provider with a request for data held by the Provider, 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.

2.5 **Subprocessors.** Provider shall enter into written agreements with all Subprocessors where the Subprocessor will have access to Data, whereby the Subprocessors agree to protect the Data in a manner consistent with the terms of this DPA.

ARTICLE 3 DUTIES OF LEA

3.1 **Privacy Compliance.** LEA shall provide Data in compliance with FERPA, COPPA, PPRA, SOPIPA, AB 1584 if applicable and all other applicable California privacy laws.

3.2 **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.

3.3 **Reasonable Precautions.** If applicable, LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services.

3.4 **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 4 DUTIES OF PROVIDER

4.1 **Privacy Compliance.** Provider shall comply with all applicable state and federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPR, SOPIPA, AB 1584 and all other California privacy laws (as applicable).

4.2 **Authorized Use.** Data provided by the LEA or collected by Provider shall be used only in connection with the Provider's products and services and/or otherwise authorized under the statutes referred to in Section 4.1, above. Provider also acknowledges and agrees that it shall not make any re-disclosure of any Data or any portion thereof, including without limitation, metadata, user content or other non-public information and/or personally identifiable information contained in the Data, without the express written consent of the LEA.

4.3 **Employee Obligation.** Provider shall require all employees and agents who have access to Data to comply with all applicable provisions of this DPA.

4.4 **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 Data and not to transfer de-identified 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, except as necessary to provide the requested products and services.

4.5 **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 Data obtained from LEA 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 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 herein authorizes Provider to maintain Data obtained from LEA beyond the time period reasonably needed to complete the

disposition. Provider shall provide written notification to LEA when the Data has been disposed. The duty to dispose of 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 Data” form, a copy of which is attached hereto as Exhibit “B”. Upon receipt of a request from the LEA, Provider will immediately provide the LEA with any specified portion of the Data within ten (10) calendar days of receipt of said request.

(a) Partial Disposal During LEA’s Use of Provider’s Products and Services. LEA may request partial disposal of Data 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 Section 2.3, above.

(b) Complete Disposal Upon Termination of LEA’s Use of Provider’s Products and Services. Upon termination of LEA’s use of Provider’s products and services, Provider shall dispose or delete all Data obtained from LEA. Prior to disposition of the data, Provider shall notify LEA in writing of its option to transfer data to a separate account, pursuant to Section 2.3, 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.

4.6 Advertising Prohibition. Provider is prohibited from using or selling 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 for the Provider’s products and services; or (d) use the Data for the development of commercial products or services, other than as necessary for Provider’s products and services. This section does not prohibit Provider from using Data for adaptive learning or customized student learning purposes.

ARTICLE 5 DATA PROVISIONS

5.1 Data Security. 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. 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 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 its employees or contractors that are performing 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 from LEA when LEA is no longer using Provider's products or services, or transfer said data to LEA or LEA's designee, according to the procedure identified in Section 4.5, above.

(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 LEA Student Data in a secure digital environment and not copy, reproduce, or transmit data obtained, except as necessary to fulfill the purpose of data requests by LEA.

(d) **Employee Training.** 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 a 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 Section 7.5, Provider shall provide the name and contact information of Provider's Security Coordinator for the Student Data received.

(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 (or have its cloud/hosting provider conduct) digital and physical periodic (no less than annual) risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner.

5.2 **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 five (5) calendar days. Provider shall follow the following process:

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.

(a) The security breach notification described above in section 5.2(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.

(b) At LEA’s discretion, the security breach notification may also include any of the following:

- i. Information about what the Provider 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.

(c) 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 required, the required responsibilities and procedures for notification and mitigation of any such data breach.

(d) 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

(e) 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.

(f) 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 6 MISCELLANEOUS

6.1 **Term.** The Provider shall be bound by this DPA for so long as the Provider maintains any Data of LEA.

6.2 **Termination.** In the event that either party seeks to terminate this DPA, they may do so by mutual written consent so long LEA is no longer using Provider's products or services. 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.

6.3 **Effect of Termination Survival.** If LEA is no longer using Provider's products or services, Provider shall destroy all of LEA's Data pursuant to Section 5.1(b), and Section 2.3, above, except to the extent that any Data must be maintained by applicable law.

6.4 **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: [Laura Assem](#)

Title: [Executive Director, Technology Services](#)

Contact Information:

lassem@rcsdk8.org

[916-771-1646](tel:916-771-1646)

The designated representative for the Provider for this Agreement is:

Name: [Chandra Roughton](#)

Title: [Administrative Program Director](#)

Contact Information: chandra@luminousmindsinc.com | [916-250-8697](tel:916-250-8697)

6.5 **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.

6.6 **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.

6.7 **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE IN WHICH THE LEA IS LOCATED, 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 THE LEA IS LOCATED FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS AGREEMENT OR THE TRANSACTIONS CONTEMPLATED HEREBY.

6.8 **Limitation on Liability.** IN NO EVENT SHALL EITHER PARTY BE LIABLE TO THE OTHER PARTY FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT, EXEMPLARY, PUNITIVE, INCIDENTAL, OR SIMILAR DAMAGES, WHETHER IN CONTRACT, TORT, OR OTHERWISE, EVEN IF SUCH DAMAGES WERE FORESEEABLE OR KNOWN BY THE PARTIES; PROVIDED, HOWEVER, THAT THE FOREGOING LIMITATION ON DAMAGES SHALL NOT APPLY TO ANY CLAIM ARISING FROM DAMAGES TO THE EXTENT CAUSED BY THE GROSS NEGLIGENCE OR WILLFUL MISCONDUCT OF THE BREACHING PARTY OR ITS EMPLOYEES, DIRECTORS, OFFICERS OR SUBCONTRACTORS. THE MAXIMUM LIABILITY OF PROVIDER

FOR ALL CLAIMS RELATING TO THE PROVIDER'S PRODUCTS AND/OR SERVICES PROVIDED TO LEA SHALL NOT EXCEED THE TOTAL AMOUNT PAID BY LEA TO PROVIDER IN THE TWELVE MONTHS PRECEDING THE EVENTS GIVING RISE TO THE CLAIM.

6.9 **Force Majeure.** Except with respect to payment obligations of LEA, neither party shall be liable for any failure or delay in performing any provision of this Agreement to the extent such failure or delay results from acts beyond the affected party's reasonable control, without such party's fault or negligence, and which by its nature could not have been foreseen or if it could have been foreseen, was unavoidable ("**Force Majeure Events**"). Force Majeure Events include without limitation, acts of God, flood, fire, earthquake, explosion, war, hostilities (whether war is declared or not), riot or other civil unrest, government order or law or other governmental action, embargoes or blockades, labor strikes, pandemics, epidemics, shortage of adequate power or transportation facilities. The party suffering a Force Majeure Event shall give notice to the other party, stating the period of time the Force Majeure Event is expected to continue and shall use diligent efforts to end the failure or delay promptly and minimize the effect of such Force Majeure Event.

6.10 **Authority.** Provider represents that it is authorized to bind to the terms of this Agreement, including confidentiality and destruction of Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Data and/or any portion thereof, or may own, lease or control equipment or facilities of any kind where the 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.

6.11 **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.

6.12 **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.

6.13 **Counterparts.** This Agreement may be executed in several counterparts, each of which so executed shall constitute one and the same instrument. A copied, scanned, electronic, or faxed signature shall be treated the same as an original signature.

[Signatures on Following Page]

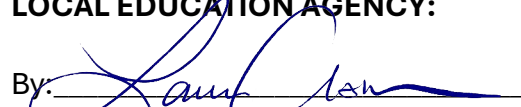
IN WITNESS WHEREOF, the parties have executed this Data Privacy Agreement as of the last day noted below.

PROVIDER:

By: Chandra Roughton
Name: Chandra Roughton
Title: Administrative Program Director

Date: 01.28.25

LOCAL EDUCATION AGENCY:

By: 
Name: Laura Assem
Title: Executive Director, Technology Services

Date: 2/5/2025

EXHIBIT “A”

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 included in the term “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. This term shall also 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 Agreement, the term “Provider” means Luminous Minds, Inc., the provider of certain educational products and services. Within the DPA the term “Provider” includes 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: 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 is certain 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 shall not constitute that information that has been anonymized or de-identified, or anonymous usage data.

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.

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.

EXHIBIT “B”

DIRECTIVE FOR DISPOSITION OF DATA

Roseville City School District (“LEA”) directs Luminous Minds, Inc. (“Provider”) to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider or otherwise in relation to LEA’s purchase and use of Provider’s Products and/or Services. The terms of the Disposition are set forth below:

Extent of Disposition 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.
Nature of Disposition 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.
Timing of Disposition Data shall be disposed of by the following date:	<input type="checkbox"/> As soon as commercially practicable <input type="checkbox"/> By (Insert Date)

Verification of Disposition of Data by:

Authorized Representative of Provider

Date