

Board Office Use: Legislative File Info.	
File ID Number	25-1078
Introduction Date	5/14/25
Enactment Number	
Enactment Date	



**OAKLAND UNIFIED
SCHOOL DISTRICT**
Community Schools, Thriving Students

Board Cover Memorandum

To Board of Education

From Kyla Johnson-Trammell, Superintendent
Jenine Lindsey, Interim General Counsel

Meeting Date May 14, 2025

Subject Software as a Service Agreement 2024-25
Contractor: Grand River Solutions
Services For: Legal Department

Ask of the Board Ratification by the Board of Education of a Software As A Service (“SaaS”) Agreement 2024-2025 and Standard Student Data Privacy Agreement, each, by and between the District and Grand River Solutions, Saratoga, CA, for the latter to provide software under the SaaS model, on a fully hosted basis, to assist in the tracking and management of discrimination and harassment complaints and resolution, for the term April 3, 2025 through June 30, 2027, in an not to exceed amount of \$24,800 per fiscal year, plus an implementation fee of \$8,000 and an annual license fee of \$8,400, for the term April 3, 2025 through June 30, 2027.

Background and Discussion Grand River Solutions has specialized expertise in Title IX investigations and training for education institutions. Their software and case tracker will streamline the process of managing, responding and resolving discrimination and harassment cases.

Competitively Bid Was this contract competitively bid? No.
If no, exception: Specialized Services (legal services).

Fiscal Impact General Purpose fund, not to exceed \$24,800 per fiscal year, plus an implementation fee of \$8,000 and an annual license fee of \$8,400.

In-Kind Contributions N/A

Attachments

- SaaS Agreement 2024-2025
- Standard Student Data Privacy Agreement



SOFTWARE AS A SERVICE (SaaS) AGREEMENT 2024-2025

This Services Agreement (“AGREEMENT”) is a legally binding contract entered into between the Oakland Unified School District (“OUSD”) and the entity or individual (“SOFTWARE PROVIDER,” together with OUSD, “PARTIES”) named in **Exhibit A**, attached hereto, and incorporated herein by reference. Unless otherwise stated herein, “SOFTWARE PROVIDER INDIVIDUAL” includes (to the extent they exist): SOFTWARE PROVIDER Board members, officers, trustees, and directors; SOFTWARE PROVIDER employees, agents, consultants, contractors and subcontractors, representatives, and other similar individuals; and volunteers and others unpaid persons under SOFTWARE PROVIDER’s direction, invitation, or control.

The PARTIES hereby agree as follows:

1. **Services.**

- a. SOFTWARE PROVIDER shall grant access to or otherwise provide the services (“SERVICES”) as described in #1A and #1B of **Exhibit A**, attached hereto and incorporated herein by reference. To the extent that there may be a school closure (e.g., due to poor air quality, planned loss of power, COVID-19) or similar event in which school sites and/or District offices may be closed or otherwise inaccessible, SOFTWARE PROVIDER shall describe in #1B of **Exhibit A** whether and how its services would be able to continue.
- b. SOFTWARE PROVIDER shall provide to Customer the necessary passwords and network links or connections to allow Customer to access the Services.
- c. SOFTWARE PROVIDER shall provide OUSD with support services to support teachers and staff with technical issues and troubleshooting throughout the course of the contract as requested by OUSD and as further outlined in **Exhibit A**.
- d. SOFTWARE PROVIDER grants such licenses and user permissions as the SOFTWARE PROVIDER offers in its end user license agreement (See **Exhibit B** if applicable) and terms of use and as OUSD may accept by Click-Wrap. If SOFTWARE PROVIDER provides an End User agreement for incorporation into this agreement, OUSD only agrees to the terms of the End User agreement as of (“October 28, 2024”) in the exact wording as they appear in Exhibit B. OUSD does not agree to any future iterations of SOFTWARE PROVIDER’S End User Agreement that occur on its website or elsewhere after (“October 28, 2024”).
- e. To the extent that any terms in License Provider’s End User agreement, Click-wrap other agreement or document, quote or invoice are in conflict with

any of the following, OUSD DOES NOT agree to any of the following:

- (i) Jurisdiction, venue, and governing law other than California.
- (ii) Indemnification by OUSD of any person.
- (iii) Binding arbitration or any other binding extra-judicial dispute resolution process.
- (iv) Waiver of jury trial.
- (v) Use or ownership of OUSD Information other than as expressly permitted in this Agreement.
- (vi) Automatic renewal of licenses, end user license agreements, terms of use, or any other contractual rights and obligations
- (vii) Insurance, Confidentiality and Liability obligations other than those found in this agreement.

2. **Term.** The term ("TERM") of this AGREEMENT is established in **Exhibit A**.

3. **Compensation.**

- a. Over the TERM, OUSD agrees to pay SOFTWARE PROVIDER the amount of money stated in **Exhibit A** for satisfactorily performing the SERVICES. OUSD shall not pay and shall not be liable to SOFTWARE PROVIDER for any costs or expenses paid or incurred by SOFTWARE PROVIDER not described in **Exhibit A**.
- b. Compensation for SERVICES performed outside of the TERM (e.g., prior to execution of this AGREEMENT or after its termination) shall be at OUSD's sole discretion and in an amount solely determined by OUSD. SOFTWARE PROVIDER agrees that it shall not expect or demand compensation for the performance of such SERVICES.
- c. SOFTWARE PROVIDER acknowledges and agrees not to expect or demand compensation for any SERVICES performed prior to the PARTIES, particularly OUSD, validly and properly executing this AGREEMENT and SOFTWARE PROVIDER shall not rely on verbal or written communication from any individual, other than the OUSD Superintendent or the OUSD Legal Counsel, stating that OUSD has validly and properly executed this AGREEMENT.
- d. SOFTWARE PROVIDER will bill OUSD upon execution of this AGREEMENT for the implementation and license fee as described in Exhibit A. Then SOFTWARE PROVIDER will continue to bill the license fee as described in Exhibit A on an annual basis for the term of the agreement. Payment is due no event later than 60 days from the presentation of the invoice. If the University has any questions about the invoice, please immediately contact GRS so that any concerns can be promptly resolved.
- e. Payment for services shall be made for all undisputed amount prior to software providers provision of services in accordance to paragraph 4 (Invoicing). The granting of any payment by OUSD, or the receipt thereof by SOFTWARE

PROVIDER, shall in no way lessen the liability of SOFTWARE PROVIDER to correct unsatisfactory performance of SERVICES, even if the unsatisfactory character of the performance was not apparent or detected at the time a payment was made. If OUSD determines that SOFTWARE PROVIDER's performance does not conform to the requirements of this AGREEMENT, SOFTWARE PROVIDER agrees to correct its performance without delay.

4. **Invoicing.** Invoices furnished by SOFTWARE PROVIDER under this AGREEMENT must be in a form acceptable to OUSD.
 - a. All amounts paid by OUSD shall be subject to audit by OUSD. Invoices shall include, without limitation: SOFTWARE PROVIDER name, SOFTWARE PROVIDER address, invoice date, invoice number, purchase order number, name of school or department to which the SERVICES were provided, name(s) of the person(s) performing the SERVICES, date(s) the SERVICES were performed, brief description of the SERVICES to be provided, total invoice amount, and the basis for the total invoice amount (e.g., if hourly rate, the number of hours on each date and the rate for those hours).
 - b. If OUSD, at its sole discretion, determines an invoice fails to include the required elements, OUSD will not pay the invoice and will inform SOFTWARE PROVIDER of the missing items; SOFTWARE PROVIDER shall resubmit an invoice that includes the required elements before OUSD will pay the invoice.
 - c. Invoices must be submitted no more frequently than monthly, and within 30 days of the conclusion of the applicable billing period. OUSD reserves the right to refuse to pay untimely invoices.
 - d. OUSD reserves the right to add or change invoicing requirements. If OUSD does add or change invoicing requirements, it shall notify SOFTWARE PROVIDER in writing and the new or modified requirements shall be mandatory upon receipt by SOFTWARE PROVIDER of such notice.
 - e. To the extent that SOFTWARE PROVIDER has described how the SERVICES may be provided both in-person and not in-person, SOFTWARE PROVIDER's invoices shall—in addition to any invoice requirement added or changed under subparagraph (d)—indicate whether the SERVICES were provided in-person or not.
 - f. All invoices furnished by SOFTWARE PROVIDER under this AGREEMENT shall be delivered to OUSD via email unless OUSD requests, in writing, a different method of delivery.
5. **Suspension.** If OUSD, at its sole discretion, develops health and safety concerns related to SOFTWARE PROVIDER's provision of SERVICES, then the OUSD Superintendent or an OUSD Chief may, upon approval by OUSD legal counsel, issue a notice to VENDOR to suspend this AGREEMENT, in which case SOFTWARE PROVIDER shall stop providing SERVICES under this AGREEMENT until further notice from OUSD. OUSD shall compensate SOFTWARE PROVIDER for the SERVICES satisfactorily provided through the date of suspension.

6. **Termination.** Upon termination consistent with this Paragraph (Termination), SOFTWARE PROVIDER shall provide OUSD with all materials produced, maintained, or collected by SOFTWARE PROVIDER pursuant to this AGREEMENT, whether or not such materials are complete or incomplete or are in final or draft form.
 - a. For Convenience by OUSD. OUSD may at any time terminate this AGREEMENT upon thirty (30) days prior written notice to SOFTWARE PROVIDER. OUSD shall compensate SOFTWARE PROVIDER for SERVICES satisfactorily provided through the date of termination. Upon approval by OUSD legal counsel, the OUSD Superintendent or an OUSD Chief may issue the termination notice without prior approval by the OUSD Governing Board, in which case this AGREEMENT would terminate upon ratification of the termination by the OUSD Governing Board or thirty (30) days after the notice was provided, whichever is later. SOFTWARE PROVIDER shall immediately stop providing SERVICES upon receipt of the termination notice from the OUSD Superintendent or OUSD Chief, consistent with data extraction described in Section 5 of Exhibit B. (Case Tracker Terms & Conditions).
 - b. For Cause. Either PARTY may terminate this AGREEMENT by giving written notice of its intention to terminate for cause to the other PARTY. Written notice shall contain the reasons for such intention to terminate, which shall include (i) material violation of this AGREEMENT or (ii) if either PARTY is adjudged bankrupt, makes a general assignment for the benefit of creditors, or a receiver is appointed on account of its insolvency. Upon approval by OUSD legal counsel, the OUSD Superintendent or an OUSD Chief may issue the termination notice without prior approval by the OUSD Governing Board, in which case this AGREEMENT would terminate upon ratification of the termination by the OUSD Governing Board or three (3) days after the notice was provided, whichever is later, unless the condition or violation ceases or satisfactory arrangements for its correction are made. SOFTWARE PROVIDER shall immediately stop providing SERVICES upon receipt of the termination notice from the OUSD Superintendent or OUSD Chief, consistent with data extraction described in Section 5 of Exhibit B. (Case Tracker Terms & Conditions).
 - c. Due to Unforeseen Emergency or Acts of God. Notwithstanding any other language of this AGREEMENT, if there is an unforeseen emergency or an Act of God during the TERM that would prohibit or limit, at the sole discretion of OUSD, the ability of SOFTWARE PROVIDER to perform the SERVICES, OUSD may terminate this AGREEMENT upon seven (7) days prior written notice to VENDOR. The OUSD Governing Board may issue this type of termination notice or the OUSD Superintendent, upon approval by OUSD legal counsel, may issue this type of the termination notice without the need for approval or ratification by the OUSD Governing Board. SOFTWARE PROVIDER shall immediately stop providing SERVICES upon receipt of the termination notice from the OUSD Superintendent.
 - d. Due to Failure to Ratify by OUSD Board. If, consistent with Paragraph 41 (Signature Authority), this AGREEMENT is executed on behalf of OUSD by the signature of the Superintendent, a Chief, a Deputy Chief, or an Executive Director,

and the Board thereafter declines to ratify this AGREEMENT, this AGREEMENT shall automatically terminate on the date that the Board declines to ratify it. OUSD shall compensate SOFTWARE PROVIDER for the SERVICES satisfactorily provided through the date of termination.

- e. **Destruction or Return of Confidential Information.** Upon expiration or termination of this Agreement for any reason, SOFTWARE PROVIDER shall promptly return to the District, or destroy, as the parties agree, all copies of OUSD students and staff Confidential Information. All copies, notes or other derivative material relating to the Confidential Information shall be promptly retrieved or destroyed, as agreed, and no such material shall be retained or used by the receiving party in any form or for any reason. This section will be consistent with section 5 of Exhibit B. (Case Tracker Terms & Conditions).

7. **Data and Information Requests.**

- a. SOFTWARE PROVIDER shall timely provide OUSD with any data and information OUSD reasonably requests related to the provision of the SERVICES.
- b. SOFTWARE PROVIDER shall register with and maintain current information within OUSD's Community Partner database unless OUSD communicates to SOFTWARE PROVIDER in writing otherwise, based on OUSD's determination that the SERVICES are not related to community school outcomes. If and when SOFTWARE PROVIDER's programs and school site(s) change (either midyear or in subsequent years), SOFTWARE PROVIDER shall promptly update the information in the database.
- c. **Sub-Processors** SOFTWARE PROVIDER shall obtain written consent from OUSD prior to engaging any Sub-Processors or other third parties to process, or otherwise access OUSD Data on Customer's behalf. Where SOFTWARE PROVIDER engages Sub-Processors or other third parties, SOFTWARE PROVIDER will impose data protection terms on the Sub-Processors that provide at least the same level of protection for OUSD Data as those in this agreement. SOFTWARE PROVIDER will remain responsible for each Sub-Processor's or third party's compliance with the obligations of this agreement.
- d. **Data breach** in the case of a data breach that includes OUSD data, SERVICE PROVIDER shall notify OUSD of such breach within 48 hours after having become aware of it. The notice shall describe the measures taken or proposed to be taken by the SOFTWARE PROVIDER to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effect shall timely provide OUSD with any data and information OUSD reasonably requests related to the provision of the SERVICES.

8. **Confidentiality and Data Privacy.**

- a. OUSD may share information with SOFTWARE PROVIDER pursuant to this AGREEMENT in order to further the purposes thereof. SOFTWARE PROVIDER and SOFTWARE PROVIDER INDIVIDUALS shall maintain the confidentiality of all information received in the course of performing the SERVICES, provided such information is (i) marked or identified as "confidential" or "privileged," or (ii) reasonably understood to be confidential or privileged.

- b. SOFTWARE PROVIDER understands that student data is confidential. SOFTWARE PROVIDER or SOFTWARE PROVIDER INDIVIDUALS may only access or receive identifiable student data, other than directory information, in connection with this AGREEMENT only after SOFTWARE PROVIDER and OUSD execute (i) a California Student Data Privacy Agreement ("CSDPA") or CSDPA Exhibit E, if SOFTWARE PROVIDER is a software vendor, or (ii) the OUSD Data Sharing Agreement, if SOFTWARE PROVIDER is not a software vendor. Notwithstanding Paragraph 24 (Indemnification), should SOFTWARE PROVIDER or SOFTWARE PROVIDER INDIVIDUALS access or receive identifiable student data, other than directory information, without first executing such an agreement, SOFTWARE PROVIDER shall be solely liable for any and all claims or losses resulting from its access or receipt of such data.
- (i) Student Records. With respect to any access by SOFTWARE PROVIDER to any "education records" (as such term is defined in the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232 et seq. ("FERPA")) held by Customer under or in connection with this Agreement, SOFTWARE PROVIDER shall be acting as a legal agent ("school official") of Customer. As between the Parties, any information protected by FERPA submitted to SOFTWARE PROVIDER by Customer in connection with this Agreement shall be deemed the Confidential Information of Customer. SOFTWARE PROVIDER agrees to comply with FERPA and agrees not to share or disclose any FERPA protected information with any third party except as permitted by FERPA or as authorized or permitted by Customer.
- c. SOFTWARE PROVIDER will use reasonable security safeguards, including but not limited to encryption and other electronic and technological measures, to prevent the use or disclosure of District Data other than as provided by this Agreement.
- d. All confidentiality requirements, including those set forth in the separate data sharing agreement, extend beyond the termination of this AGREEMENT.
9. **Copyright/Trademark/Patent/Ownership.** Except for any intellectual property owned by SOFTWARE PROVIDER that existed prior to execution of this AGREEMENT, SOFTWARE PROVIDER understands and agrees that all other matters produced under this AGREEMENT shall be works for hire as defined under Title 17 of the United States Code, and all copyrights in those works are the property of OUSD. These matters include, without limitation, drawings, plans, specifications, studies, reports, memoranda, computation sheets, the contents of computer diskettes, artwork, copy, posters, billboards, photographs, videotapes, audiotapes, systems designs, software, reports, diagrams, surveys, source codes or any other original works of authorship, or other documents prepared by SOFTWARE PROVIDER in connection with the SERVICES performed under this AGREEMENT. SOFTWARE PROVIDER cannot use, reproduce, distribute, publicly display, perform, alter, remix, or build upon matters produced under this AGREEMENT without OUSD's express written permission. OUSD shall have all right, title and interest in said matters, including the right to register the copyright, trademark,

and/or patent of said matter in the name of OUSD. OUSD may, with SOFTWARE PROVIDER's prior written consent, use SOFTWARE PROVIDER's name in conjunction with the sale, use, performance and distribution of the matters, for any purpose and in any medium.

- a. SOFTWARE PROVIDER. As between SOFTWARE PROVIDER and Customer, all right, title and interest in the software and any other SOFTWARE PROVIDER materials furnished or made available hereunder, including all copyright rights, patent rights and other intellectual property rights in the software and materials provided by SOFTWARE PROVIDER, belong to and are retained solely by SOFTWARE PROVIDER.
 - b. OUSD Data. As between SOFTWARE PROVIDER and Customer, all right, title and interest in (i) the OUSD Data, (ii) other information input into Case Tracker by Customer (collectively, "Other Information") and (iii) all intellectual property rights in each of the foregoing, belong to and are retained solely by Customer.
10. **Alignment and Evaluation.**
 - a. SOFTWARE PROVIDER agrees to work and communicate with OUSD staff, both formally and informally, to ensure that the SERVICES are aligned with OUSD's mission and are meeting the needs of students as determined by OUSD.
 - b. OUSD may evaluate SOFTWARE PROVIDER or SOFTWARE PROVIDER INDIVIDUALS in any reasonable manner which is permissible under the law. OUSD's evaluation may include, without limitation: (i) requesting that OUSD employee(s) evaluate the performance of SOFTWARE PROVIDER or SOFTWARE PROVIDER INDIVIDUALS, and (ii) announced and unannounced observance of SOFTWARE PROVIDER or SOFTWARE PROVIDER INDIVIDUALS.
11. **Inspection and Approval.** SOFTWARE PROVIDER agrees that OUSD has the right and agrees to provide OUSD with the opportunity to inspect any and all aspects of the SERVICES performed including, but not limited to, any materials (physical or electronic) produced, created, edited, modified, reviewed, or otherwise used in the preparation, performance, or evaluation of the SERVICES. In accordance with Paragraph 3 (Compensation), the SERVICES performed by SOFTWARE PROVIDER must meet the approval of OUSD, and OUSD reserves the right to direct SOFTWARE PROVIDER to redo the SERVICES, in whole or in part, if OUSD, in its sole discretion, determines that the SERVICES were not performed in accordance with this AGREEMENT.
12. **Equipment and Materials.** SOFTWARE PROVIDER shall provide all equipment, materials, and supplies necessary for the performance of this AGREEMENT.
13. **Legal Notices.** Based on contact information set forth in **Exhibit A**, all legal notices provided for under this AGREEMENT shall be sent: (i) via email, (ii) personally delivered during normal business hours, or (iii) sent by U.S. Mail (certified, return receipt requested) with postage prepaid to the other PARTY. Notice shall be effective when

received if personally served or emailed or, if mailed, three days after mailing. Either PARTY must give written notice of a change of mailing address or email.

14. **Status.**

- a. This is not an employment contract. SOFTWARE PROVIDER, in the performance of this AGREEMENT, shall be and act as an independent contractor.
- b. If SOFTWARE PROVIDER is a natural person, SOFTWARE PROVIDER verifies all of the following:
 - (i) SOFTWARE PROVIDER is free from the control and direction of OUSD in connection with SOFTWARE PROVIDER's work;
 - (ii) SOFTWARE PROVIDER's work is outside the usual course of OUSD's business; and
 - (iii) SOFTWARE PROVIDER is customarily engaged in an independently established trade, occupation, or business of the same nature as that involved in the work performed for OUSD.
- c. If SOFTWARE PROVIDER is a business entity, SOFTWARE PROVIDER understands and agrees that it and any and all VENDOR INDIVIDUALS shall not be considered employees of OUSD, and are not entitled to benefits of any kind or nature normally provided employees of OUSD and/or to which OUSD's employees are normally entitled, including, but not limited to, State Unemployment Compensation or Worker's Compensation. SOFTWARE PROVIDER shall assume full responsibility for payment of all Federal, State, and local taxes or contributions, including unemployment insurance, social security and income taxes with respect to VENDOR INDIVIDUALS. SOFTWARE PROVIDER verifies all of the following:
 - (i) SOFTWARE PROVIDER is free from the control and direction of OUSD in connection with the performance of the work;
 - (ii) SOFTWARE PROVIDER is providing the SERVICES directly to OUSD rather than to customers of OUSD;
 - (iii) the contract between OUSD and SOFTWARE PROVIDER is in writing;
 - (iv) SOFTWARE PROVIDER has the required business license or business tax registration, if the work is performed in a jurisdiction that requires SOFTWARE PROVIDER to have a business license or business tax registration;
 - (v) SOFTWARE PROVIDER maintains a business location that is separate from the business or work location of OUSD;
 - (vi) SOFTWARE PROVIDER is customarily engaged in an independently established business of the same nature as that involved in the work performed;
 - (vii) SOFTWARE PROVIDER actually contracts with other businesses to provide the same or similar services and maintains a clientele without restrictions from OUSD;
 - (viii) SOFTWARE PROVIDER advertises and holds itself out to the public as available to provide the same or similar services;

- (ix) SOFTWARE PROVIDER provides its own tools, vehicles, and equipment to perform the SERVICES;
- (x) SOFTWARE PROVIDER can negotiate its own rates;
- (xi) SOFTWARE PROVIDER can set its own hours and location of work; and
- (xii) SOFTWARE PROVIDER is not performing the type of work for which a license from the Contractor's State License Board is required, pursuant to Chapter 9 (commencing with section 7000) of Division 3 of the Business and Professions Code.

15. Qualifications, Training, and Removal.

- a. SOFTWARE PROVIDER represents and warrants that SOFTWARE PROVIDER and all SOFTWARE PROVIDER INDIVIDUALS have the necessary and sufficient experience, qualifications, and ability to perform the SERVICES in a professional manner, without the advice, control or supervision of OUSD. SOFTWARE PROVIDER will perform the SERVICES in accordance with generally and currently accepted principles and practices of its profession for services to California school districts and in accordance with applicable laws, codes, rules, regulations, and/or ordinances.
- b. SOFTWARE PROVIDER represents and warrants that all VENDOR INDIVIDUALS are specially trained, experienced, competent and fully licensed to provide the SERVICES identified in this AGREEMENT in conformity with the laws and regulations of the State of California, the United States of America, and all local laws, ordinances and/or regulations, as they may apply.
- c. SOFTWARE PROVIDER agrees to immediately remove or cause the removal of any VENDOR INDIVIDUAL from OUSD property upon receiving notice from OUSD of such desire. OUSD is not required to provide SOFTWARE PROVIDER with a basis or explanation for the removal request.

- 16. Certificates/Permits/Licenses/Registration.** SOFTWARE PROVIDER shall ensure that all SOFTWARE PROVIDER INDIVIDUALS secure and maintain in force such certificates, permits, licenses, and registration as are required by law in connection with the furnishing of the SERVICES pursuant to this AGREEMENT. SOFTWARE PROVIDER warrants that it has the right to provide access to the Software Application to OUSD pursuant to this Agreement, that Service Provider has obtained any and all necessary permissions from third parties to provide the Software Application, and that use of the Software Application by Authorized Users in accordance with the terms of this Agreement shall not infringe the copyright of any third party.

17. Insurance.

- a. **Commercial General Liability Insurance.** SOFTWARE PROVIDER shall maintain Commercial General Liability Insurance, including automobile coverage, with limits of at least one million dollars (\$1,000,000) per occurrence, and two million dollars (\$2,000,000) aggregate, sexual misconduct, harassment, bodily injury and

property damage. Coverage for corporal punishment, sexual misconduct, and harassment may either be provided through General Liability Insurance or Professional Liability Insurance. The coverage shall be primary as to OUSD and shall name OUSD as an additional insured with the additional insured endorsement provided to OUSD within 15 days of effective date of this AGREEMENT (and within 15 days of each new policy year thereafter during the TERM). Evidence of insurance shall be attached to this AGREEMENT or otherwise provided to OUSD upon request. Endorsement of OUSD as an additional insured shall not affect OUSD's rights to any claim, demand, suit or judgment made, brought or recovered against SOFTWARE PROVIDER. The policy shall protect SOFTWARE PROVIDER and OUSD in the same manner as though each were separately issued. Nothing in said policy shall operate to increase the Insurer's liability as set forth in the policy beyond the amount or amounts shown or to which the Insurer would have been liable if only one interest were named as an insured. The requirements of this subparagraph may be specifically waived as noted in **Exhibit A**.

- b. **Workers' Compensation Insurance.** SOFTWARE PROVIDER shall procure and maintain, at all times during the TERM of this AGREEMENT, Workers' Compensation Insurance in conformance with the laws of the State of California (including, but not limited to, Labor Code section 3700) and Federal laws when applicable. Employers' Liability Insurance shall not be less than one million dollars (\$1,000,000) per accident or disease. The requirements of this subparagraph may be specifically waived as noted in **Exhibit A**.
18. **Testing and Screening.**
- a. **Tuberculosis Screening.** If applicable, SOFTWARE PROVIDER shall ensure that all SOFTWARE PROVIDER INDIVIDUALS who will be working at OUSD sites for more than six hours in total during the TERM or who work with students (regardless of the length of time) have submitted to a tuberculosis risk assessment as required by Education Code section 49406 within the prior 60 days. If tuberculosis risk factors were identified for a SOFTWARE PROVIDER INDIVIDUAL, that SOFTWARE PROVIDER INDIVIDUAL must submit to an intradermal or other approved tuberculosis examination to determine if that SOFTWARE PROVIDER INDIVIDUAL is free of infectious tuberculosis. If the results of the examination are positive, SOFTWARE PROVIDER shall obtain an x-ray of the lungs. SOFTWARE PROVIDER, at its discretion, may choose to submit a SOFTWARE PROVIDER INDIVIDUAL to the examination instead of the risk assessment. The requirements of this subparagraph may be specifically waived as noted in **Exhibit A**.
 - b. **Fingerprinting/Criminal Background Investigation.** If applicable, for all SOFTWARE PROVIDER INDIVIDUALS providing the SERVICES, SOFTWARE PROVIDER shall ensure completion of fingerprinting and criminal background investigation and shall request and regularly review subsequent arrest records. SOFTWARE PROVIDER confirms that no SOFTWARE PROVIDER INDIVIDUAL providing the SERVICES has been convicted of a felony, as that term is defined in

Education Code section 45122.1. SOFTWARE PROVIDER shall provide the results of the investigations and subsequent arrest notifications to OUSD. For purposes of this subparagraph, SOFTWARE PROVIDER shall use either California Department of Justice or Be A Mentor, Inc. (<http://beamentor.org/OUSDPartner>) finger-printing and subsequent arrest notification services. The requirements of this subparagraph may be specifically waived as noted in **Exhibit A**.

19. Incident/Accident/Mandated Reporting.

- a. SOFTWARE PROVIDER shall notify OUSD, via email pursuant to Paragraph 13 (Legal Notices), within twelve (12) hours of learning of any significant accident or incident in connection with the provision of the SERVICES. Examples of a significant accident or incident include, without limitation, an accident or incident that involves law enforcement, or possible or alleged criminal activity, or possible or actual exposure to a communicable disease such as COVID-19. SOFTWARE PROVIDER shall properly submit required accident or incident reports within one business day pursuant to the procedures specified by OUSD. SOFTWARE PROVIDER shall bear all costs of compliance with this Paragraph.
- b. To the extent that a SOFTWARE PROVIDER INDIVIDUAL is included on the list of mandated reporters found in Penal Code section 11165.7, SOFTWARE PROVIDER agrees to inform that SOFTWARE PROVIDER INDIVIDUAL, in writing, that they are a mandated reporter, and describing the associated obligations to report suspected cases of abuse and neglect pursuant to Penal Code section 11166.5.

20. Health and Safety Orders and Requirements; Site Closures.

- a. SOFTWARE PROVIDER shall adhere to any health or safety orders or requirements issued at the time of the execution of this AGREEMENT or in the future by OUSD or other public entities ("Orders").
- b. Except as possibly stated otherwise in **Exhibit A**, SOFTWARE PROVIDER is able to meet its obligations and perform the SERVICES required pursuant to this AGREEMENT in accordance with any Order; to the extent that SOFTWARE PROVIDER becomes unable to do so, SOFTWARE PROVIDER shall immediately inform OUSD in writing.
- c. Except as possibly stated otherwise in **Exhibit A**, to the extent that there may be a site closure (e.g., due to poor air quality, planned loss of power, strike) or similar event in which school sites and/or District offices may be closed or otherwise inaccessible, SOFTWARE PROVIDER is able to meet its obligations and perform the SERVICES required pursuant to this AGREEMENT; to the extent that SOFTWARE PROVIDER becomes unable to do so, SOFTWARE PROVIDER shall immediately inform OUSD in writing.
- d. SOFTWARE PROVIDER shall bear all costs of compliance with this Paragraph, including but not limited lost compensation for failure to provide SERVICES.

21. Conflict of Interest.

- a. SOFTWARE PROVIDER and all SOFTWARE PROVIDER INDIVIDUALS shall abide by and be subject to all applicable, regulations, statutes, or other laws regarding conflict of interest. VENDOR shall not hire, contract with, or employ any officer or employee of OUSD during the TERM without the prior approval of OUSD Legal Counsel.
 - b. SOFTWARE PROVIDER affirms, to the best of his/her/its knowledge, that there exists no actual or potential conflict of interest between SOFTWARE PROVIDER's family, business, or financial interest and the SERVICES provided under this AGREEMENT, and in the event of any change in either private interest or the SERVICES under this AGREEMENT, any question regarding a possible conflict of interest which may arise as a result of such change will be immediately brought to OUSD's attention in writing.
 - c. Through its execution of this AGREEMENT, SOFTWARE PROVIDER acknowledges that it is familiar with the provisions of section 1090 *et seq.* and section 87100 *et seq.* of the Government Code, and certifies that it does not know of any facts which constitute a violation of said provisions. In the event SOFTWARE PROVIDER receives any information subsequent to execution of this AGREEMENT which might constitute a violation of said provisions, SOFTWARE PROVIDER agrees it shall immediately notify OUSD in writing.
22. **Certification Regarding Debarment, Suspension, Ineligibility and Voluntary Exclusion.** SOFTWARE PROVIDER certifies, to the best of its knowledge and belief, that it and its principals are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by any Federal department or agency according to Federal Acquisition Regulation Subpart 9.4, and by signing this AGREEMENT, certifies that neither it nor its principals appear on the Excluded Parties List (<https://www.sam.gov/>).
23. **Limitation of OUSD Liability.** Other than as provided in this AGREEMENT, OUSD's financial obligations under this AGREEMENT shall be limited to the compensation described in Paragraph 3 (Compensation). Notwithstanding any other provision of this AGREEMENT, in no event shall OUSD be liable, regardless of whether any claim is based on contract or tort, for any special, consequential, indirect or incidental damages, including, but not limited to, lost profits or revenue, arising out of, or in connection with, this AGREEMENT for the SERVICES performed in connection with this AGREEMENT.
24. **Indemnification.**
 - a. To the furthest extent permitted by California law, SOFTWARE PROVIDER shall indemnify, defend and hold harmless OUSD, its Governing Board, agents, representatives, officers, consultants, employees, trustees, and volunteers ("OUSD Indemnified Parties") from any and all claims or losses accruing or resulting from injury, damage, or death of any person or entity arising out of SOFTWARE PROVIDER's performance of this AGREEMENT. SOFTWARE PROVIDER also agrees to hold harmless, indemnify, and defend OUSD Indemnified Parties

from any and all claims or losses incurred by any supplier or subcontractor furnishing work, services, or materials to SOFTWARE PROVIDER arising out of the performance of this AGREEMENT. SOFTWARE PROVIDER shall, to the fullest extent permitted by California law, defend OUSD Indemnified Parties at SOFTWARE PROVIDER's own expense, including attorneys' fees and costs, and OUSD shall have the right to accept or reject any legal representation that SOFTWARE PROVIDER proposes to defend OUSD Indemnified Parties.

- b. To the furthest extent permitted by California law, OUSD shall indemnify, defend, and hold harmless SOFTWARE PROVIDER and SOFTWARE PROVIDER INDIVIDUALS from any and all claims or losses accruing or resulting from injury, damage, or death of any person or entity arising out of OUSD's performance of this AGREEMENT. OUSD shall, to the fullest extent permitted by California law, defend SOFTWARE PROVIDER and SOFTWARE PROVIDER INDIVIDUALS at OUSD's own expense, including attorneys' fees and costs.
25. **Audit.** SOFTWARE PROVIDER shall establish and maintain books, records, and systems of account, in accordance with generally accepted accounting principles, reflecting all business operations of SOFTWARE PROVIDER transacted under this AGREEMENT. SOFTWARE PROVIDER shall retain these books, records, and systems of account during the TERM and for three (3) years after the earlier of (i) the TERM or (ii) the date of termination. SOFTWARE PROVIDER shall permit OUSD, its agent, other representatives, or an independent auditor to audit, examine, and make excerpts, copies, and transcripts from all books and records, and to make audit(s) of all billing statements, invoices, records, and other data related to the SERVICES covered by this AGREEMENT. Audit(s) may be performed at any time, provided that OUSD shall give reasonable prior notice to SOFTWARE PROVIDER and shall conduct audit(s) during SOFTWARE PROVIDER'S normal business hours, unless SOFTWARE PROVIDER otherwise consents.
26. **Non-Discrimination.** It is the policy of OUSD that, in connection with all work performed under legally binding agreements, there be no discrimination because of race, color, ancestry, national origin, religious creed, physical disability, medical condition, marital status, sexual orientation, gender, or age; therefore, SOFTWARE PROVIDER agrees to comply with applicable Federal and California laws including, but not limited to, the California Fair Employment and Housing Act beginning with Government Code section 12900 and Labor Code section 1735 and OUSD policy. In addition, SOFTWARE PROVIDER agrees to require like compliance by all its subcontractor (s). SOFTWARE PROVIDER shall not engage in unlawful discrimination in employment on the basis of actual or perceived: race, color, national origin, ancestry, religion, age, marital status, pregnancy, physical or mental disability, medical condition, veteran status, gender, sex, sexual orientation, or other legally protected class.
27. **Drug-Free/Smoke Free Policy.** No drugs, alcohol, and/or smoking are allowed at any time in any buildings and/or grounds on OUSD property. No students, staff, visitors,

SOFTWARE PROVIDER, or subcontractors are to use controlled substances, alcohol or tobacco on these sites.

28. **Waiver.** No delay or omission by either PARTY in exercising any right under this AGREEMENT shall operate as a waiver of that or any other right or prevent a subsequent act from constituting a violation of this AGREEMENT.
29. **Assignment.** The obligations of SOFTWARE PROVIDER under this AGREEMENT shall not be assigned by SOFTWARE PROVIDER without the express prior written consent of OUSD and any assignment without the express prior written consent of OUSD shall be null and void.
30. **No Rights in Third Parties.** This AGREEMENT does not create any rights in, or inure to the benefit of, any third party except as expressly provided herein.
31. **Litigation.** This AGREEMENT shall be deemed to be performed in Oakland, California and is governed by the laws of the State of California, but without resort to California's principles and laws regarding conflict of laws. The Alameda County Superior Court shall have jurisdiction over any litigation initiated to enforce or interpret this AGREEMENT.
32. **Incorporation of Recitals and Exhibits.** Any recitals and exhibits attached to this AGREEMENT are incorporated herein by reference. SOFTWARE PROVIDER agrees that to the extent any recital or document incorporated herein conflicts with any term or provision of this AGREEMENT, the terms and provisions of this AGREEMENT shall govern.
33. **Integration/Entire Agreement of Parties.** This AGREEMENT constitutes the entire agreement between the PARTIES and supersedes all prior discussions, negotiations, and agreements, whether oral or written. This AGREEMENT may be amended or modified only by a written instrument executed by both PARTIES.
34. **Severability.** If any term, condition, or provision of this AGREEMENT is held by a court of competent jurisdiction to be invalid, void or unenforceable, the remaining provisions will nevertheless continue in full force and effect, and shall not be affected, impaired or invalidated in any way.
35. **Provisions Required By Law Deemed Inserted.** Each and every provision of law and clause required by law to be inserted in this AGREEMENT shall be deemed to be inserted herein and this AGREEMENT shall be read and enforced as though it were included therein.
36. **Captions and Interpretations.** Paragraph headings in this AGREEMENT are used solely for convenience, and shall be wholly disregarded in the construction of this AGREEMENT. No provision of this AGREEMENT shall be interpreted for or against a PARTY because that

PARTY or its legal representative drafted such provision, and this AGREEMENT shall be construed as if jointly prepared by the PARTIES.

37. **Calculation of Time.** For the purposes of this AGREEMENT, "days" refers to calendar days unless otherwise specified and "hours" refers to hours regardless of whether it is a work day, weekend, or holiday.
38. **Counterparts and Electronic Signature.** This AGREEMENT, and all amendments, addenda, and supplements to this AGREEMENT, may be executed in one or more counterparts, all of which shall constitute one and the same amendment. Any counterpart may be executed and delivered by facsimile or other electronic signature (including portable document format) by either PARTY and, notwithstanding any statute or regulations to the contrary (including, but not limited to, Government Code section 16.5 and the regulations promulgated therefrom), the counterpart shall legally bind the signing PARTY and the receiving PARTY may rely on the receipt of such document so executed and delivered electronically or by facsimile as if the original had been received. Through its execution of this AGREEMENT, each PARTY waives the requirements and constraints on electronic signatures found in statute and regulations including, but not limited to, Government Code section 16.5 and the regulations promulgated therefrom.
39. **W-9 Form.** If SOFTWARE PROVIDER is doing business with OUSD for the first time, VENDOR acknowledges that it must complete and return a signed W-9 form to OUSD.
40. **Agreement Publicly Posted.** This AGREEMENT, its contents, and all incorporated documents are public documents and will be made available by OUSD to the public online via the Internet.
41. **Signature Authority.**
 - a. Each PARTY has the full power and authority to enter into and perform this AGREEMENT, and the person(s) signing this AGREEMENT on behalf of each PARTY has been given the proper authority and empowered to enter into this AGREEMENT.
 - b. Notwithstanding subparagraph (a), SOFTWARE PROVIDER acknowledges, agrees, and understands (i) that only the Superintendent, and the Chiefs, Deputy Chiefs, and Executive Directors who have been delegated such authority, may validly sign contracts for OUSD and only under limited circumstances, and (ii) that all such contract still require ratification by the OUSD Governing Board. SOFTWARE PROVIDER agrees not to accept the signature of another other individual as having the proper authority to enter into this AGREEMENT on behalf of OUSD.
42. **Contract Contingent on Governing Board Approval.** The PARTIES acknowledge, agree, and understand that OUSD shall not be bound by the terms of this AGREEMENT unless and until it has been (i) formally approved by OUSD's Governing Board or (ii) validly and properly executed by the OUSD Superintendent, a Chief, or a Deputy Chief authorized by

the Education Code or Board Policy, and no compensation shall be owed or made to SOFTWARE PROVIDER absent such formal approval or valid and proper execution.

REST OF PAGE INTENTIONALLY LEFT BLANK

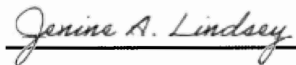
IN WITNESS WHEREOF, the PARTIES hereto agree and execute this AGREEMENT and to be bound by its terms and conditions:

SOFTWARE PROVIDER

Name: Jody Shipper Signature: 
Jody Shipper (03 April, 2025 15:01:32 UTC)
 Position: Managing Director Date: April 03, 2025

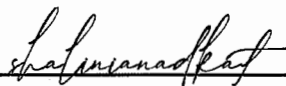
One of the terms and conditions to which VENDOR specifically agrees by its signature is subparagraph (c) of Paragraph 3 (Compensation), which states that VENDOR acknowledges and agrees not to expect or demand compensation for any SERVICES performed prior to the PARTIES, particularly OUSD, validly and properly executing this AGREEMENT and shall not rely on verbal or written communication from any individual, other than the OUSD Superintendent or OUSD Legal Counsel, stating that OUSD has validly and properly executed this AGREEMENT.

OUSD

Name: Jenine Lindsey Signature: 
 Position: General Counsel Date: 04/15/25
☐ Board President (for approvals)
☒ Chief/Deputy Chief/Executive Director (for ratifications)

Name: Kyla Johnson-Trammell Signature: _____
 Position: Superintendent Date: _____

Approved as to form by OUSD Legal Department

Name: Shalini Anadkat Signature:  Date: 4/2/2025

**SERVICES AGREEMENT
EXHIBIT A**

(Paragraph numbers in Exhibit A corresponds to the applicable Paragraph number in this Agreement.)

VENDOR: Grand River Solutions

1A. Services. Describe the SERVICES VENDOR will provide: GRS has developed a proprietary product that is a secure, online platform that, among other features, connects parties to appropriate portions of their resolution process, allows parties to communicate with the institutional office responsible for those processes, and tracks the status of and documents and communications related to a complaint receipt and resolution process. The Terms & Conditions for this product are attached and incorporated herein.

See attached Case Tracker Proposal for Case Tracker Premium

1B. General Description of Support Services to be Provided: *This includes the protocol for OUSD to request support services. As per Exhibit B, Client will receive updates to support changes to the GRS System. GRS will provide online technical support for all system users through the Product. Additionally, Lead Client Contact(s) may receive direct electronic mail and telephone support.*

1. Term.

- a. This AGREEMENT shall start on the below Start Date. If no date is entered, then this AGREEMENT shall start on the latest of the dates on which each of the PARTIES signed this AGREEMENT.

Start Date: 4/3/2025

- b. Unless terminated earlier, this AGREEMENT shall end on the below End Date. If no date is entered, then this AGREEMENT shall end on the first June 30 after start date listed in subparagraph (a). If the dates set forth in this subparagraph and subparagraph (a) would cause this AGREEMENT to exceed the limits set forth in state law (e.g., Education Code section 17596), this AGREEMENT shall instead automatically end upon reaching said limit.

End date: 6/30/2027

2. **Compensation.**

- a. The basis for payment to VENDOR shall be:
- ☐ Hourly Rate: _____ per hour
 - ☐ Daily Rate: _____ per day
 - ☐ Weekly Rate: _____ per week
 - ☐ Monthly Rate: _____ per month
 - ☐ Per Student Served Rate: _____ per student served
 - ☒ Performance/Deliverable Payments: Describe below the performance and/or deliverable(s) as well as the associated rate(s): Implementation Fee: \$8000
Annual License Fee: \$8400
- b. Over the TERM, the total compensation under this AGREEMENT shall not exceed the below amount. This sum includes (but is not limited to) compensation for the full performance of this AGREEMENT and all fees, costs, and expenses incurred by VENDOR including (but not limited to) labor, materials, taxes, profit, overhead, travel, insurance, permitted subcontractor costs, and other costs.
Not-To-Exceed Amount: \$24,800.00_____

13. **Legal Notices.**

OUSD

Site/Dept: Legal Department
Address: 1011 Union Street, Site 946
City, ST Zip: Oakland, CA 94607
Phone: 510-879-5060
Email: ousdlegal@ousd.org

VENDOR

Name/Dept: Grand River Solutions
Address: PO Box 2094
City, ST Zip: Saratoga, CA 95070
Phone: _____
Email: _____

17. **Insurance.** OUSD has waived the following insurance requirements. Written confirmation of a waiver (e.g., email from OUSD Risk Management Officer) is attached hereto. Failure to attach such written confirmation voids any such waiver even if otherwise properly given.

- ☐ *Commercial General Liability Insurance.* Waiver typically available by OUSD if no VENDOR INDIVIDUAL interacts or has contact with OUSD students (in-person or virtual) and the not-to-exceed amount is \$25,000 or less.
- ☐ *Workers' Compensation Insurance.* Waiver typically available by OUSD if VENDOR has no employees.

18. **Testing and Screening.** OUSD has waived the following testing and screening requirements. Written confirmation of a waiver (e.g., email from OUSD Risk Management Officer) is attached hereto. Failure to include such written confirmation voids any such waiver even if otherwise properly given.
- ☒ *Tuberculosis Screening.* Waiver typically available by OUSD if VENDOR INDIVIDUALS will have no in-person contact with OUSD students.
 - ☒ *Fingerprinting/Criminal Background Investigation.* typically available by OUSD if no VENDOR INDIVIDUAL interacts or has contact with OUSD students (in-person or virtual).
20. **Health and Safety Orders and Requirements; Site Closures.** If there is an Order or event in which school sites and/or District offices may be closed or otherwise inaccessible, would the SERVICES be able to continue?
- ☒ Yes, the SERVICES would be able to continue as described herein. ☐ No, the SERVICES would not be able to continue.

Exhibit B
Case Tracker Terms & Conditions

These Terms & Conditions ("Terms") accompany the Agreement for Services between OAKLAND UNIFIED SCHOOL DISTRICT ("Client") and Grand River Solutions ("GRS"), together the "Parties." The Agreement between the Parties authorizes GRS to provide the Services and the Client agrees to pay the associated fees. Client refers to the institution named above and "GRS" refers to Grand River Solutions, together they are referred to as the "Parties." In the event of a conflict between Exhibit B and the clauses in the above agreement, the clauses in the above agreement shall govern.

These terms may be updated by GRS only with express written agreement by OUSD to the new terms.

1. Service.

GRS offers software provided under the Software-as-a-Service (SaaS) model, on a fully hosted basis to assist in the tracking and management of discrimination and harassment complaints and resolution processes.

GRS will establish and maintain an Internet based system (commonly referred to as "Case Tracker" or the "GRS System"), a secure, online and mobile platform that, among other features, connects parties to appropriate portions of their resolution process, allows parties to communicate with the institutional office responsible for those processes, and tracks the status of documents and communications related to a complaint receipt and resolution process. Client retains sole ownership and remains the custodian of all institutional records stored in the GRS System, whether created by the Client's employee or submitted or uploaded by a user. GRS will provide and maintain the systems established to provide this service. Pending implementation, as described in in these Terms, the system shall provide the following functions: (i) allow Client to create and maintain case files regarding incidents; (ii) allow Client to generate and store necessary documentation and correspondence related to cases; (iii) allow Client to generate statistical summaries derived from the Client's information in the database; (iv) allow Client to draw pre-defined demographic data from the Client's people information systems into the GRS System where technically feasible when creating a new case; (v) allow Client's staff to access the GRS System electronically via a tiered permissions system with local access controlled and granted by the Client; and (vi) allow Client's faculty, staff, students, or nonaffiliate participants in Client resolution processes to access the GRS System electronically via a specialized portal with local access controlled and granted by the Client.

2. Implementation.

After the mutual execution of the Agreement between GRS and the Client, including these Terms, the Parties will engage in the implementation process. The Client will designate at least one employee with administrative privileges to maintain the system, including setting permissions of other users (sometimes called a "superuser"). The Client will also designate at least one employee as a Lead Client Contact responsible for implementation of Case Tracker. The Parties will have an initial meeting where GRS will notify the Client of what information and materials are required in order to customize Case Tracker ("Onboarding Information"). The Client will timely provide the required Onboarding Information to GRS, and the Parties will mutually agree upon the implementation schedule, including timeline for customization, delivery, and training. GRS will then customize Case Tracker according to the Onboarding Information and in consultation with the Client as needed. GRS will deliver Case Tracker to the Lead Client Contact(s). Substantial modifications after Product delivery may be charged at an hourly rate as per the terms of this Agreement, depending on the Client's license level. All costs associated with implementation are included in the Implementation Fee specified in this Agreement, and are non-refundable. Costs associated with implementation shall be at least wholly or partially refundable in limited cases where the contract must terminate due to issues related to the provisions of paragraph 6b and 6c in this contract within the first three months of service. GRS will provide remote training for Client's staff users, including superusers, which will take place over approximately one and a half days at a mutually agreed upon time.

3. Technical Support.

Client will receive updates to support changes to the GRS System. GRS will provide online technical support for all system users through the Product. Additionally, Lead Client Contact(s) may receive direct electronic mail and telephone support.

4. Encryption & Backup.

Data stored in Client's GRS System will be backed up and encrypted nightly. This encrypted backup will then be transmitted over a secure channel to a geographically separate server for storage. Backups will be retained on a rolling approximate thirty (30) day cycle. GRS warrants that both its primary and backup servers upon which Client's data is stored are and will continue to be located in the United States. GRS employs a contractor, NMX Global Software, Inc. to assist with software engineering and client onboarding. NMX is a United States Company headquartered in California that employs personnel in the United States and offshore. All personnel, regardless of location, are subject to policies on security, privacy, and the United States laws regarding such, are regularly trained and attest to their compliance with such policies and practices which are, in all cases, at least as protective as those that the Client would use in similar situations.

5. Termination of Services.

If the Services are terminated, GRS will make the Client's records in the GRS System available no later than thirty (30) business days (or promptly if the data and/or records fall under paragraph 6e of this agreement) from termination of services. The parties will mutually agree upon the method of transfer for the records. If the parties fail to reach a mutual agreement about the method and timing of transfer, in all such circumstances GRS will transfer the records using a

commercially available secure system to the established Lead Client Contact. If the Lead Client Contact is unavailable or unresponsive, the records will be provided to the most senior administrative office of the Client's organization, such as the office of the President. Once the transfer is complete, and in all instances within ninety (90) days of termination of services, Client's records will no longer be maintained in the system or by GRS. Upon request, GRS will provide a certificate of destruction.

6. Data Feeds.

If applicable, the parties acknowledge that properly working data feeds from Client's information systems are essential to the Services and that the absence of such would significantly hinder the practical functionality of the system, which may result in inconvenience to Client and unfair reputational damage to GRS. The parties acknowledge their obligation for mutual cooperation under their Agreement includes maintaining the data feeds.

7. Limited License

Subject to these Terms, GRS grants Client a limited, non-exclusive, nontransferable license to use GRS's relevant Intellectual Property during the term of the Agreement between the Parties solely for Client's own internal purposes. Client shall not sell, market, rent, or re-license any aspect of the Intellectual Property. Client obtains no ownership rights or any other rights in the Intellectual Property, other than those specified herein. Client grants GRS a license to use Client's non-confidential, non-personally identifiable information (e.g., statistical information) on a consolidated basis as part of GRS's overall statistics for marketing and/or analytical purposes as long as such use is consistent with the terms of the accompanying data sharing agreement. GRS grants Client license to use the GRS and Case Tracker names and logos on its website or materials used to display compliance or related. Neither license implies endorsement. Client is the owner of all substantive documents that it creates or which are submitted to it in the course of using the software (including, for example, evidence in a matter, the names and information about the party, the investigation report), and GRS takes no license or ownership in such information. This paragraph shall be consistent with the terms of paragraph 9 above in the agreement.

8. Marketing & Publicity

GRS shall not use in its external advertising, marketing programs, publicity or other promotional efforts, whether such efforts are paid strategies or unpaid earned strategies, any data, visual depictions (including photographic, video and animated images), or other representation of the Client except on the specific, written authorization in advance by OUSD.

9. Using the Client's Name, Logo, Trademarks or Other Identifying Marks

GRS recognizes and acknowledges that all rights and goodwill in the Client's name, logo, trademarks and other identifying marks are the exclusive property of the Client. GRS may include the Client's name, logo or other identifying marks on its website or other media with

prior written permission and final proof approval from OUSD. Such use must comply with the Client's brand standards, including allowable logo usage as outlined by OUSD. The Client reserves the right to terminate GRS's license or permission for such use at any time and without cause being stated.

10. Affiliation

Client may announce its affiliation with the GRS on its website or other media in a manner deemed mutually acceptable to both Parties.

11. Data Security.

Grand River Solutions utilizes a Data Management policy that requires multiple login stages, multi-factor authentication, and complex passwords. Grand River Solutions does not store any data locally, but relies on encrypted, commercially available products for data storage and transfer. Grand River Solutions has a protocol and maintains insurance for breach and breach notification.

Client and its personnel that are receiving or transferring information or data to or from Grand River Solutions is/are responsible for protecting their account credentials, using complex and non-repeated passwords, maintaining the security of their devices, and notifying Grand River Solutions of a breach under which an unauthorized person, persons, or organization(s) may have access to their password or other relevant information in accordance with the terms of this agreement.

Upon Client's reasonable request, GRS shall provide access to documentation of GRS's data security plans and practices relevant to the Services under these Terms. Client agrees that all such documentation is Confidential Information, as defined in the Agreement between the Parties, and Client further agrees not to disclose such documentation or any of its content without the express written permission of GRS.

12. Accessibility.

GRS takes commercially reasonable and available steps to ensure that the GRS System is accessible under the law and to the level of industry best practice.

15. Client's Responsibility.

GRS customizes and, if applicable, modifies the GRS System consistent with instructions by the Client. GRS makes no guarantees about whether Client's policies or procedures, in general, or as applied in any specific case, comply with applicable laws or whether Client's actions comply with Client's published policies. Client is responsible for granting and managing access to Case Tracker in a way that is consistent with applicable laws including but not limited to the Children's Online Privacy Protection Act. Client is responsible for protecting user account credentials.

16. GRS's Limited Liability.

Liability will be in accordance with the terms of this agreement.

Nothing in this section – GRS's Limited Liability, or elsewhere in this Agreement, shall limit GRS's liability to the Client or third-parties that:

- (1) arise from personal injury, death, or property damage or loss caused by vendor's negligence or willful misconduct or
- (2) are covered by GRS's indemnification obligations under this agreement.
- (3) are connected to events indicating that data with personally identifiable information that was sent, received or stored by GRS may have been accessed, disclosed, or acquired without proper authorization in connection with the services that GRS is providing Client under this Agreement.

End of Case Tracker Terms & Conditions

STANDARD STUDENT DATA PRIVACY AGREEMENT

**CA-NDPA Standard
Version 1.5
(01.28.25)**

Oakland Unified School District

and

Grand River Solutions

This Student Data Privacy Agreement (“**DPA**”) is entered into on the date of full execution (the “**Effective Date**”) and is entered into by and between:

Oakland Unified School District , located at 1011 Union St. Oakland, CA Suite 946 94607
(the “**Local Education Agency**” or “**LEA**”) and

Grand River Solutions , located at P.O. Box 2094, Saratoga, CA 95070
(the “**Provider**”).

WHEREAS, the Provider is providing educational or digital services to LEA.

WHEREAS, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act (“**FERPA**”) at 20 U.S.C. § 1232g (34 CFR Part 99); the Children’s Online Privacy Protection Act (“**COPPA**”) at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations
and

WHEREAS, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.

NOW THEREFORE, for good and valuable consideration, LEA and Provider agree as follows:

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.

2. **Special Provisions. *Check if Required***

If checked, the Supplemental State Terms and attached hereto as **Exhibit “G”** are hereby incorporated by reference into this DPA in their entirety.

☒ If Checked, the Provider, has signed **Exhibit “E”** to the Standard Clauses, otherwise known as General Offer of Privacy Terms

3. In the event of a conflict between the SDPC Standard Clauses, the State or Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this DPA shall control.
4. This DPA shall stay in effect for three years. Exhibit E will expire 3 years from the date the original DPA was signed.
5. The services to be provided by Provider to LEA pursuant to this DPA are detailed in **Exhibit “A”** (the “**Services**”).
6. **Notices**. All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or first-class mail, sent to the designated representatives below.

The designated representative for the LEA for this DPA is:

Name: Jenine Lindsey Title: ene nse

Address: 1011 Union St. Oakland, CA Suite 946 94607

Phone: _____ Email: enine lindsey sd

The designated representative for the Provider for this DPA is:

Name: Jody Shipper Title: Co-Founder & Managing Direct

Address: P.O. Box 2094, Saratoga, CA 95070

Phone: (650) 383-4753 Email: jshipper@grandriversolutions.com

IN WITNESS WHEREOF, LEA and Provider execute this DPA as of the Effective Date.

LEA: Oakland Unified School District

By: Jenine A. Lindsey Date: _____

Printed Name: Jenine Lindsey Title/Position: ene nse

PROVIDER: Grand River Solutions

By: Jody Shipper Date: April 03, 2025

Jody Shipper (03 April, 2025 15:02:14 UTC)

Printed Name: Jody Shipper Title/Position: Co-Founder & Managing Dire

STANDARD CLAUSES

Version 3.0

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 including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, 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. Provider shall be under the direct control and supervision of the LEA, with respect to its use of Student Data
2. **Student Data to Be Provided.** In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit “B”**.
3. **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 terms used in any other writing, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies etc.

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 DPA 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 LEA as it pertains to the use of Student Data, notwithstanding the above.
2. **Parent Access.** To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than forty five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA's request for Student Data in a student's records held by the Provider to view or correct as necessary. In the event that a parent of a student 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 Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student-Generated Content to a separate account created by the student.

4. **Law Enforcement Requests.** Should law enforcement or other government entities (“Requesting Party(ies)”) contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.
5. **Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws.** LEA shall provide Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.
2. **Annual Notification of Rights.** If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA (34 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 Student Data.
4. **Unauthorized Access Notification.** LEA shall notify Provider promptly of any known 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 federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.
2. **Authorized Use.** The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in Exhibit A or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA.
3. **Provider Employee Obligation.** Provider shall require all of Provider’s employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Student Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.
4. **No Disclosure.** Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non-public information and/or personally identifiable information contained in the Student Data other than as directed or

permitted by the LEA or this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not Sell Student Data to any third party.

5. **De-Identified Data**: Provider agrees not to attempt to re-identify de-identified Student Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; and (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Except for Subprocessors, Provider agrees 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 the LEA who has provided prior written consent for such transfer. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which de-identified data is presented.
6. **Disposition of Data**. Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to section II 3. The LEA may employ a "Directive for Disposition of Data" form, a copy of which is attached hereto as **Exhibit "D"**. If the LEA and Provider employ Exhibit "D," no further written request or notice is required on the part of either party prior to the disposition of Student Data described in Exhibit "D."
7. **Advertising Limitations**. Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits

ARTICLE V: DATA PROVISIONS

1. **Data Storage**. Where required by applicable law, Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.
2. **Audits**. No more than once a year, or following unauthorized access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA . The Provider will cooperate reasonably with the LEA and any local, state, or federal

agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA. Failure to reasonably cooperate shall be deemed a material breach of the DPA.

3. **Data Security.** The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The provider shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth set forth in **Exhibit "F"**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment to **Exhibit "H"**. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit "F"**. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.
4. **Data Breach.** In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:
 - (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:
 - 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; and
 - v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
 - (2) Provider agrees to adhere to all federal and state requirements 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.
 - (3) 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 summary of said written incident response plan.

- (4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians.
- (5) 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 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 **Exhibit "E"** to any other LEA who signs the acceptance on said Exhibit. The form is limited by the terms and conditions described therein.

ARTICLE VII: MISCELLANEOUS

1. **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. Either party may terminate this DPA and any service agreement or contract if the other party breaches any terms of this DPA.
2. **Effect of Termination Survival.** If the Service Agreement is terminated, the Provider shall destroy all of LEA's Student Data pursuant to Article IV, section 6.
3. **Priority of Agreements.** This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between Exhibit H, the SDPC Standard Clauses, and/or the Supplemental State Terms, Exhibit H will control, followed by the Supplemental State Terms. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.
4. **Entire Agreement.** This DPA and the Service Agreement constitute 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.

5. **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. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE LEA, 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 OF THE LEA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.
7. **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. In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement. The LEA has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.
8. **Authority.** Each party represents that it is authorized to bind to the terms of this DPA, 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.
9. **Waiver.** No delay or omission by either party to exercise any right hereunder shall be construed as a waiver of any such right and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

EXHIBIT "A"
DESCRIPTION OF SERVICES

GRS has developed a proprietary product that is a secure, online platform that, among other features, connects parties to appropriate portions of their resolution process, allows parties to communicate with the institutional office responsible for those processes, and tracks the status of and documents and communications related to a complaint receipt and resolution process. Further described in Proposal for Case Tracker Premium

Unless specified, and explicitly excluded below, this DPA covers access to and use of all Provider's Services, as well as any future Services that Provider may offer. This coverage extends, without limitation, to all subdomains, software, mobile applications, and products that are owned and operated by Provider, its subsidiaries, and/or affiliates, except for those explicitly excluded below.

If applicable, any **EXCLUDED** services will be listed below and are therefore not covered by this DPA:

I have completed **Exhibit "A"** and, if applicable, specified any excluded Services that are not covered under this DPA.

EXHIBIT B: SCHEDULE OF STUDENT DATA

All Data Elements identified in this Exhibit are correct at time of signature.

Data Elements Collected by Product (required and optional):

Category of Data / Data Elements	ALL DPA- COVERED APPS						
Application Technology MetaData							
IP Addresses of users, use of cookies, etc.	X						
Other application technology metadata							
<i>If 'Other' checked, please specify below checked box:</i>							
Application Use Statistics							
Meta data on user interaction with application	X						
Assessment							
Standardized test scores							
Observation data							
Voice recordings							
Other assessment data							
<i>If 'Other' checked, please specify below checked box:</i>							
Attendance							
Student school (daily) attendance data							

Category of Data / Data Elements	ALL DPA- COVERED APPS						
Student class attendance data							
Communication							
Online communication captured (emails, blog entries)	X						
Conduct							
Conduct or behavioral data	X						
Demographics							
Data of birth	X						
Place of birth	X						
Gender	X						
Ethnicity or race	X						
Language information (native, or primary language spoken by student)	X						
Other demographic information							
<i>If 'Other' checked, please specify below checked box:</i>							
Enrollment							
Student school enrollment	X						
Student grade level	X						
Homeroom	X						
Guidance counselor	X						
Specific curriculum programs	X						
Year of graduation	X						

Category of Data / Data Elements	ALL DPA- COVERED APPS						
Other enrollment information							
<i>If 'Other' checked, please specify below checked box:</i>							
Parent/Guardian Contact Information							
Address	X						
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							
Special Indicator							
English language learner information	X						
Low-income status	X						
Medical alerts/health data	X						
Student disability information	X						
Specialized education Services (IEP or 504)	X						
Living situations (homeless/foster care)	X						
Other indicator information	X						

Category of Data / Data Elements	ALL DPA- COVERED APPS						
<i>If 'Other' checked, please specify below checked box:</i>							
Student Contact Information							
Address	X						
Email	X						
Phone	X						
Student Identifiers							
Local (school district) ID number	X						
State ID number	X						
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/application performance (e.g. typing program – student types 60 wpm, reading program – student reads below grade level)	X						
Student Program Membership							
Academic or extracurricular activities a student may belong to or participate in	X						

Category of Data / Data Elements	ALL DPA- COVERED APPS						
Student Survey Responses							
Student responses to surveys or questionnaires							
Student Work							
Student generated content; writing, pictures, etc.	X						
Other student work data							
<i>If 'Other' checked, please specify below checked box:</i>							
Transcript							
Student course grades							
Student course data							
Student course grades/performance scores							
Other transcript data							
<i>If 'Other' checked, please specify below checked box:</i>							
Transportation							
Student bus assignment							
Student pick up and/or drop off location							
Student bus card ID number							
Other transportation data							

Category of Data / Data Elements	ALL DPA- COVERED APPS						
<i>If 'Other' checked, please specify below checked box:</i>							
Other							
Other data collected							
<i>If 'Other' checked, please list each additional data element used, stored, or collected by your application below checked box:</i>							
None							
No student data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.							

EXHIBIT "C"

DEFINITIONS

De-Identified Data and De-Identification: Records and information are considered to be de-identified when all personally identifiable information has been removed or obscured, such that the remaining information does not reasonably identify a specific individual, including, but not limited to, any information that, alone or in combination is linkable to a specific student and provided that the educational agency, or other party, has made a reasonable determination that a student's identity is not personally identifiable, taking into account reasonable available information.

Educational Records: Educational Records are records, files, documents, and other materials directly related to a student and maintained by the school or local education agency, or by a person acting for such 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.

Metadata: means information that provides meaning and context to other data being collected; including, but not limited to: date and time records and purpose of creation Metadata that have been stripped of all direct and indirect identifiers are not considered Personally Identifiable Information.

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 for K-12 school purposes. Any entity that operates an internet website, online service, online application, or mobile application that has entered into a signed, written agreement with an LEA to provide a service to that LEA shall be considered an "operator" for the purposes of this section.

Originating LEA: An LEA who originally executes the DPA in its entirety with the Provider.

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

Student Generated Content: The term "student-generated content" means materials or content created by a student in the services 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 student content.

School Official: For the purposes of this DPA 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 Student Data including Education Records; and (3) Is subject to 34 CFR § 99.33(a) governing the use and re-disclosure of personally identifiable information from Education Records.

Service Agreement: Refers to the Contract, Purchase Order or Terms of Service or Terms of Use.

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, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or 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, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data includes Meta Data. Student Data further includes "personally identifiable information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local 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.

Subprocessor: For the purposes of this DPA, 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 service, and who has access to Student Data.

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

Targeted Advertising: means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the operator's Internet web site, online service or mobile application by such student or the retention of such student's online activities or requests over time for the purpose of targeting subsequent advertisements. "Targeted advertising" does not include any advertising to a student on an Internet web site based on the content of the web page or in response to a student's response or request for information or feedback.

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 Education Records and/or Student Data, as that term is used in some state statutes. However, for the purpose of this DPA, 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

Provider 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:

1. Extent of Disposition

_____ Disposition is partial. The categories of data to be disposed of are set forth below or are found in an attachment to this Directive:

_____ Disposition is complete. Disposition extends to all categories of data.

2. Nature of Disposition

_____ Disposition shall be by destruction or deletion of data.

_____ Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

3. Schedule of Disposition

Data shall be disposed of by the following date:

_____ As soon as commercially practicable.

_____ By _____

4. Signature

Authorized Representative of LEA

Date

5. Verification of Disposition of Data

Authorized Representative of Company

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

Oakland Unified School District

("Originating LEA") which is dated _____, to any other LEA ("Subscribing LEA") who accepts this General Offer of Privacy Terms ("General Offer") through its signature below. This General Offer shall extend only to privacy protections, and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the Subscribing LEA may also agree to change the data provided by Subscribing LEA to the Provider to suit the unique needs of the Subscribing 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 listed in the originating Service Agreement; or three (3) years after the date of Provider's signature to this Form. Subscribing LEAs should send the signed **Exhibit "E"** to Provider at the following email address:

info@grandriversolutions.com

PROVIDER: Grand River Solutions

Jody Shipper

BY: Jody Shipper (02 April 2025 15:00:14 UTC) Date: April 03, 2025

Printed Name: Jody Shipper Title/Position: Co-Founder & Managing Director

2. Subscribing LEA

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

and the Provider. ****PRIOR TO ITS EFFECTIVENESS, SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER PURSUANT TO ARTICLE VII, SECTION 5. ****

LEA: nd ni ied is i

BY: Jenine A. Lindsey Date: _____

Printed Name: Jenine Lindsey Title/Position: ene nse

SCHOOL DISTRICT NAME: nd ni ied is i

DESIGNATED REPRESENTATIVE OF LEA:

Name: Jenine Lindsey

Title: ene nse

Address: ni n ee nd

Telephone Number: _____

Email: enine lindsey sd

EXHIBIT "F"
DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks
2/24/2020

Below is a list of known and credible cybersecurity frameworks which can protect digital learning ecosystems chosen based on a set of guiding cybersecurity principles ("Cybersecurity Frameworks") that may be utilized by Provider.

Cybersecurity Frameworks

	MAINTAINING ORGANIZATION/GROUP	FRAMEWORK(S)
	National Institute of Standards and Technology	NIST Cybersecurity Framework Version 1.1
	National Institute of Standards and Technology	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
	International Standards Organization	Information technology – Security techniques – Information security management systems (ISO 27000 series)
	Secure Controls Framework Council, LLC	Security Controls Framework (SCF)
	Center for Internet Security	CIS Critical Security Controls (CSC, CIS Top 20)
	Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S))	Cybersecurity Maturity Model Certification (CMMC, ~FAR/DFAR)

Case Tracker is designed to meet or exceed the principles of ISO 27000 Series Cybersecurity framework. We are on track to obtain SOC 2 certification in 2025.

Case Tracker employs four security monitoring services to log API calls, track configuration changes, automatically detect threats, and provide a centralized view of these logs. These security services include continuous monitoring for threats. Moreover, Grand River Solutions only utilizes software requiring multifactor authentication (this includes Case Tracker).

There are encrypted backups which occur nightly, and the transmission of that data occurs over a secure channel (SSL) to a geographically separate server; this is fully handled by the capabilities in AWS. Likewise, primary and backup servers upon which

EXHIBIT G: Supplemental State Terms for California & AI Addendum

This Amendment for State Terms for California ("**Amendment**") is entered into on the date of full execution (the "**Effective Date**") and is incorporated into and made a part of the Student Data Privacy Agreement ("**DPA**") by and between:

Oakland Unified School District, located at 1011 Union St. Oakland, CA Suite 946 94607
(the "**Local Education Agency**" or "**LEA**") and
Grand River Solutions, located at P.O. Box 2094, Saratoga, CA 95070
(the "**Provider**").

All capitalized terms not otherwise defined herein shall have the meaning as defined in the attached DPA.

WHEREAS, the Provider is providing educational or digital Services to LEA.

WHEREAS, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. §1232g (34 C.F.R. Part 99); and the Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. §6501-6506 (16 C.F.R. Part 312), applicable laws, and

WHEREAS, the Provider and LEA agree that additional and modified sections are required to address the use of Artificial Intelligence ("AI") as part of the services or product provided; and

WHEREAS, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.

NOW THEREFORE, for good and valuable consideration, LEA and Provider agree to the following:

1. **Term**. Unless otherwise terminated by the Parties, this Amendment shall remain effective for the duration of the attached DPA.
2. **Amendment to ARTICLE II, § 2**. of the DPA (Parent, Legal Guardian and Student Access) is amended as follows:

In accordance with California Education Code § 49073.1(b)(2), should the Provider store or maintain Student-Generated Content, the Provider shall, upon request from the LEA, provide a mechanism for students to retain ownership of the content they create, which shall include text or images generated by Artificial Intelligence, to be defined below. Furthermore, this NDPA does not impede the ability of students to download, export, or otherwise save or maintain their own Student Generated Content directly from Provider or for Provider to provide a mechanism for such download, export, transfer or saving to students, or the student's parent or legal guardian. Nor does it impede the ability of Providers to offer LEAs features to allow such ability.

3. **Amendment to ARTICLE I, to include the addition(s) of § 4 & 4.1 & 4.2:**

4. **Use of Artificial Intelligence**. If the Services described in Exhibit "A" require Provider to use AI, ownership of Student Data shall remain with the District or Student. The Provider is prohibited from using or reproducing Student Data for AI training or content generation without prior written consent from the District. Furthermore, sub-licensing Student Data for these purposes is strictly prohibited without explicit written permission from the parents or eligible pupils. Access to District-provided Student Data is limited to authorized users unless granted in writing by the LEA or otherwise permitted under this DPA.

4.1 Hallucinations. Provider will provide notice in the event that any feature of the services it provides is modified to include AI functions. Provider further represents that it will monitor the Hallucination rate of the service and take industry standard methods to reduce Hallucination rates.

4.2 Collection of Student Data and AI Use. The Provider must complete the attached AI Schedule of Data.

4. **Amendment to Article IV, to add a new Section 8**

8. **Algorithmic Biases.** The Provider certifies that any AI technologies used in facilitating the Services are regularly audited for biases and fairness and, if necessary, Provider shall implement strategies to identify and mitigate any discriminatory effects or biases in AI decision-making. Upon request by the LEA, the Provider shall provide the LEA an abstract or summary of findings of that portion of the audit pertaining to algorithmic bias.

Furthermore, Student Data, as defined elsewhere in the DPA, shall not be used for training purposes or to develop synthetic and/or inferred data. All other provisions of the DPA shall remain in effect.

5. **Amendment to Exhibit C: Definitions shall be amended to include the following terms:**

Algorithmic Bias: Where an algorithm produces systematically prejudiced outcomes favoring certain groups or disadvantaging others based on characteristics like gender, race, age, ethnicity or other protected attributes.

Artificial Intelligence (AI): Refers to systems that display intelligent behavior by analyzing their environment and taking action, with some degree of autonomy, to achieve specific goals.

Hallucination: A response by an artificial intelligence to a user request or query that is incorrect, nonsensical or misleading that may appear to be factually correct.

Describe how Student Data is Used:

Any other information related to Provider's use of AI:

The Provider certifies that any AI technologies used in facilitating the Services are regularly audited for biases and fairness and, if necessary, Provider shall implement strategies to identify and mitigate any discriminatory effects or biases in AI decision-making. Furthermore, Student Data, as defined elsewhere in the DPA, shall not be used for training purposes or to develop synthetic and/or inferred data. All other provisions of the DPA shall remain in effect.

IN WITNESS WHEREOF, LEA and Provider execute this DPA as of the Effective Date.

LEA: Oakland Unified School District

BY: Jenine A. Lindsey DATE: _____

Printed Name Jenine Lindsey Title/Position ene nse

Provider: Grand River Solutions

BY: _____ DATE: _____

Printed Name Jody Shipper Title/Position Co-Founder & Managing Director

AI Addendum

(METHODS EMPLOYED BY THE AI)

The following information correlates to how the Provider will use AI in the delivery services to LEA.

Type of AI Used	Description/Common Uses	Optional	Required
Intelligent Tutoring Systems/agents (ITS)	<i>Personalized instruction based on students' individual learning needs and progress</i>	☐	☐
Adaptive Learning/Assessment Platforms	<i>Adjusts the difficulty level and content of learning materials based on the student's performance and learning pace</i>	☐	☐
Natural Language Processing (NLP)	<i>Analyze and understand students' written or spoken responses, providing feedback or assistance in language learning tasks.</i>	☐	☐
Machine Learning-based Recommended Systems	<i>Recommend educational resources, such as books, videos, or exercises, based on students' preferences, learning styles, and performance history.</i>	☐	☐
Virtual Assistants (i.e. Alexa, Siri, Merlyn Mind)	<i>Provide automated and personalized support by handling tasks, answering questions, and managing workflows.</i>	☐	☐
Chatbots/LLMs (i.e. ChatGPT)	<i>Facilitate automated and interactive communication; provides instant responses to questions and assists with various tasks through natural language processing.</i>	☐	☐
Data Analytics and Predictive Modeling	<i>Analyze historical data and identify patterns to forecast future trends and inform strategic decision-making.</i>	☐	☐
Gamification and/or Personalized Learning Paths	<i>Enhance engagement and optimize individual learning experiences by incorporating game-like elements and/or tailoring educational content to each learner's unique needs and progress.</i>	☐	☐
Computer Vision (i.e. CNNs, GANs)	<i>Interpret, analyze, and generate visual data, mimicking human visual perception for applications such as image recognition, object detection, and image synthesis.</i>	☐	☐
Recommender Systems/Filtering (i.e. KNN, TF-IDF)	<i>Analyze user preferences and behavior to suggest personalized content, products, or services</i>	☐	☐
Translation (i.e. Transformer, DeepL)	<i>Translate text from one language to another, leveraging advanced machine-learning techniques to understand and generate human-like language translations.</i>	☐	☐
Neural Machine Translation (NMT)	<i>Algorithms used to provide accurate and fluent translations by understanding and processing entire sentences as opposed to individual words or phrases.</i>	☐	☐
Speech Recognition (i.e. DNNs, Wav2Vec)	<i>Convert spoken language into text by accurately identifying and processing the acoustic signals of human speech.</i>	☐	☐

Type of AI Used	Description/Common Uses	Optional	Required
Time Series Analysis (i.e. ARIMA, LSTMs)	Analyze and interpret temporal data points to identify patterns, trends, and seasonal variations, aiding in forecasting and decision-making.	☐	☐
Reinforcement Learning (i.e. Q-Learning, DQNs)	Teaches optimal behaviors and decision-making policies by interacting with an environment and receiving feedback through rewards and penalties.	☐	☐
Dimensionality Reduction i.e. (PCA, t-SNE)	Reduces the number of variables in a dataset while preserving as much variability and information as possible to simplify analysis and visualization.	☐	☐
Other Types of AI Used	Specify other types of AI here:	☐	☐
Purpose of AI Use	Description	Optional	Required
Personalized learning	Customized learning to match a students' strengths, weaknesses, and learning styles.	☐	☐
Enhanced Teaching and Learning	Assist teachers in delivering more effective instruction and help students grasp difficult concepts more easily.	☐	☐
Automated Grading and Feedback	Automate the grading for assignments, quizzes, and exams; provides immediate feedback to students.	☐	☐
Identifying Learning Gaps	Analyze student performance data to identify areas where students are struggling and provide targeted interventions to address learning gaps.	☐	☐
Supporting Special Education	Additional support and accommodations for students with special needs, including personalized learning plans and assistive technologies	☐	☐
Promoting Engagement and Motivation	Gamification elements and interactive learning experiences; increase student engagement and motivation	☐	☐
Administrative Support	Assist with administrative tasks such as scheduling, grading, and managing educational resources	☐	☐
Parental Engagement	Provide parents with insights into their student's academic progress, for communication and collaboration between parents, students, and teachers	☐	☐
Other Purpose(s) for AI Use	Specify other purpose(s) for AI here:	☐	☐

Student Data Collected With Use of AI	Description	Optional	Required
Student Name	<i>First and/or Last</i>	☐	☐
Date of Birth	<i>Student's date of birth</i>	☐	☐
Student ID Numbers	<i>Unique identification numbers to students for record-keeping purposes.</i>	☐	☐
Demographic Information	<i>Gender, race, ethnicity, nationality, language spoken at home, etc.</i>	☐	☐
Academic Records	<i>academic performance, grades, attendance, disciplinary history, etc.</i>	☐	☐
Special Education Information	<i>Individualized education plans (IEPs), accommodations, special needs, etc.</i>	☐	☐
Health Information	<i>Physical or mental health conditions, medications, allergies, medical history, etc.</i>	☐	☐
Biometric Data	<i>Fingerprints, facial recognition, or voiceprints for authentication or identification</i>	☐	☐
Behavioral Data	<i>Behavior, interactions with educational materials, engagement levels, learning preferences, etc.</i>	☐	☐
Location Information	<i>Track locations, GPS-enabled devices, attendance tracking systems, etc.</i>	☐	☐
Input Data	<i>Information fed into an AI model or algorithm, which is used to train, validate, and test the model to make predictions or perform specific tasks.</i>	☐	☐
Other Student Data	<i>Specify other Student Data here:</i>	☐	☐
No AI used at this time	<i>Provider will immediately notify LEA if this designation is no longer applicable.</i>	☐	☐

☐ All requested AI Elements have been identified in this Exhibit and are correct at time of signature.