

Board Office Use: Legislative File Info.	
File ID Number	25-1713
Introduction Date	8/13/25
Enactment Number	
Enactment Date	



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

# Board Cover Memorandum

**To** Board of Education

**From** Denise G. Saddler, EdD, Interim Superintendent  
Preston Thomas, Chief Systems and Services Officer  
Susan Beltz, Chief Technology Officer

**Meeting Date** August 13, 2025

**Subject** Ratification by the Board of Education of Customer Agreement between Oakland Unified School District and Volt, Inc.; Ratification of Data Privacy Agreement between Oakland Unified School District and Volt, Inc.  
Contractor: Volt, Inc.  
Services For: January 20, 2025 - September 17, 2025

---

**Ask of the Board** Ratification by the Board of Education of Customer Agreement between the District and Volt, Inc., Bethesda, MD, for the latter to provide software to enhance security after hours and during weekends, with existing camera feeds, for the period of January 20, 2025 through September 17, 2025 at a cost of \$27,584; Ratification of Data Privacy Agreement between Oakland Unified School District and Volt, Inc.

**Background** After hours, during weekends, and school vacation periods, many district campuses have been targets for coordinated thefts. Given the limited ability of the District, City, and contracted staff to be available to monitor and respond to potential issues during these time periods, the District is exploring options to detect perimeter breaches using virtual software tools, so that staff time and resources can be saved and only deployed in the cases of active situations. Based upon the previous successful pilot, which was approved by the Board as Legistar File ID #24-3056, OUSD is continuing to use the software at the three locations included in the no-cost pilot and will extend to a fourth location, where only staff are present during normal working hours.

**Discussion** Building on the overall work over the past several years to improve the District's safety and security, this extension will allow the District to leverage new technology tools to help mitigate safety and security issues at our campuses, particularly after normal working hours. Prior to any further renewal in September, staff will evaluate the ongoing needs at the existing locations and consider potential new locations that can benefit from this approach.

The solution provided by Volt, Inc. is currently only used at central office locations where students are typically not present. However, in the event that the solution is broadened in the future to include school sites, the camera feeds monitored by Volt, Inc. would include student activity, warranting a data privacy agreement. Accordingly, the District and Volt, Inc. executed the enclosed data sharing agreement on 06/18/2025, and now ask the Board to ratify this agreement.

This data sharing agreement is the standard California - National Student Data Privacy Agreement (CA-NDPA), adopted by the California Student Privacy Alliance to meet the requirements of the Family Educational Rights and Privacy Act (FERPA) and Assembly Bill 1584 (which allows school districts to share data with software providers so long as the contracts include certain specified provisions).

The standard terms of the CA-NDPA ensure that the vendor will take all precautions to safeguard our students' data. The term of the CA-NDPA is the same as the term of the underlying services agreement.

The CA-NDPA is a piggy-backable agreement. This means that a software vendor may enter the CA-NDPA with one school district and thereafter, by signing Exhibit E (which consists of a "general offer of terms") allow any other school district to countersign Exhibit E and be entitled to the same protections set forth in the underlying CA-NDPA.

Here, Volt, Inc. has signed the CA-NDPA with the Oakland Unified School District, and it further signed Exhibit E, which, again, allows any other school district to likewise sign Exhibit E and share the same data with Aeries, Software, Inc. under the same terms. Accordingly, the District signed the CA-NDPA on 06/18/2025, and now asks the Board to ratify this agreement.

**Fiscal Impact**

\$27,584 from 2024-25 Funding Resource 010-0000-0-0000-7700-5846-999-9860-9994-9999-99999: General Purpose (GP), Data Processing, License Agreements, Districtwide

**Attachment(s)**

- Customer Agreement
- Sales Order 2025-00012 (Services 1/20/2025 to 3/16/2025)
- Sales Order 2025-00013 (Services 3/17/2025 to 9/17/2025)
- Volt, Inc. California National Student Data Privacy Agreement with Exhibit E

## Customer Agreement

This Customer Agreement (the “**Agreement**”) is between Volt, Inc., a Delaware corporation (“**Company**”) and Oakland Unified School District (“**Customer**”).

### 1. SERVICE AND RESTRICTIONS

- 1.1 **Service.** Company and Customer may enter into one or more order forms (each, an “**Order**”) for Company’s service and/or product (the “**Service**”). Each Order will describe the Service configuration Company will provide, any usage restrictions related to Customer’s use of the Service, the applicable subscription term for the Service (the “**Subscription Term**”), and the fees and payment terms associated with that Order. Upon execution by the parties, each Order is incorporated into this Agreement. Subject to Customer’s compliance with this Agreement, Company shall provide Customer with access to the Service (in the configuration identified in the Order) during the Subscription Term for Customer’s internal business purposes. Company shall provide Customer with access information and account credentials for the Service, which are Company’s Confidential Information (as defined below). Customer’s use of the Service is limited to the configuration set forth in each Order with respect to applicable locations and the number of managed cameras or other devices at such locations. If Customer desires to change the configuration of the Service or modify any usage restrictions, the parties must enter into a new Order. To the extent Company and Customer have entered into a pilot or evaluation agreement with respect to the Service prior to the Effective Date (a “**Prior Agreement**”), such Prior Agreement is terminated.
- 1.2 **Company Equipment.** As part of the Service, Customer shall permit Company or its representatives to install on Customer’s premises Company’s hardware, equipment or other tangible materials (collectively, “**Company Equipment**”) that is required for the Service to operate. Title to any Company Equipment provided to Customer by Company in connection with this Agreement shall remain with Company. Company retains the right to replace, modify, or remove the Company Equipment at any point during the Subscription Term. Customer shall maintain Company Equipment in accordance with Company’s documentation and guidelines and protect it from damage, misuse, loss, or destruction. Customer may only use Company Equipment in connection with its use of the Service. Customer is responsible for any damage, misuse, loss, or destruction of Company Equipment except to the extent such damage, misuse, loss or destruction is caused by Company. Promptly following termination of this Agreement, Customer shall return Company Equipment to Company at Company’s expense in accordance with Company’s written instructions.
- 1.3 **Restrictions.** Customer shall not, and shall not permit, authorize, or assist any third party to: (1) modify, adapt, translate, reverse engineer, decompile, disassemble, or attempt to derive the source code of any part of the Service or Company Equipment; (2) use or integrate the Service or Company Equipment with any software, hardware, or system other than Customer’s computer equipment on which the Service is designed to

operate; (3) sell, resell, license, sublicense, distribute, rent or lease any part of the Service or Company Equipment or provide any third party with access to the Service or Company Equipment; (4) disclose to any third party any results of any benchmark or other performance tests of the Service; (5) remove, alter, or obscure any proprietary rights notices contained in or affixed to the Service or Company Equipment; (6) copy, frame, or mirror any part of the Service; (7) attempt to disrupt, degrade, impair, or violate the integrity or security of the Service, including, without limitation, by executing any form of network monitoring; (8) interfere with or disrupt the integrity or performance of the Services or the data contained therein or (9) use the Service to store or transmit any malicious code. Company may monitor Customer's use of the Service and may suspend any use of the Service that Company determines to be or reasonably believes may be in violation of the foregoing restrictions; provided, however, that prior to suspending any provision of the Service, Company may provide Customer with written notice of the violation or suspected violation and Customer shall have the opportunity to cure such violation (if curable) during the 30-day period following receipt of such notice.

- 1.4 **Export Restrictions; Government Rights.** Customer may not remove or export from the United States or allow the export or re-export of the Service, Company Equipment, or anything related thereto, or any direct product thereof in violation of any restrictions, laws or regulations of the United States Department of Commerce, the United States Department of Treasury Office of Foreign Assets Control, or any other United States or foreign agency or authority. Company provides the Service and Company Equipment, including related software and technology, that may be delivered to a federal government end user, for ultimate federal government end use solely in accordance with the following: Government technical data and software rights related to the Service include only those rights customarily provided to the public as specified in this Agreement. This customary commercial license is provided in accordance with FAR 12.211 (Technical Data) and FAR 12.212 (Software) and, for Department of Defense transactions, DFAR 252.227- 7015 (Technical Data – Commercial Items) and DFAR 227.7202-3 (Rights in Commercial Computer Software or Computer Software Documentation). If a governmental agency has a need for rights not granted under this Agreement, it must negotiate with Company to determine if there are acceptable terms for granting those rights, and a mutually acceptable written addendum specifically granting those rights must be included in any applicable agreement.
- 1.5 **No Protected Information.** Customer agrees that it shall not disclose to Company or process or submit via the Service any information that is: (1) "personal health information," as defined under the Health Insurance Portability and Accountability Act of the United States of America; (2) government-issued identification numbers, including Social Security numbers, driver's license numbers and other state or national issued identification numbers; (3) financial account information; (4) payment card data; (5) biometric information; or (6) "sensitive" personal data, as defined under Directive 95/46/EC of the European Parliament and any national laws adopted pursuant thereto.

- 1.6 **Use of Data; Customer Data.** Company may collect technical and usage data in connection with Customer's use of the Service (the "**Usage Data**"). Any such Usage Data is owned by the Company and Company may use and exploit it in any manner without restriction. Customer agrees that Company may also use video footage from Customer's use of the Service to train Company's AI Models. For purposes of this Agreement, AI Models means a machine-based system, tool or model that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as content, predictions, recommendations or decisions that influence physical or virtual environments (including an artificial intelligence model that is trained on broad data at scale, is designed for generality of output, and can be adapted to a wide range of distinctive tasks). Customer retains ownership of any data or other information input into the Service by Customer, including video records of Customer personnel and facilities, as well as mapping data (collectively, "**Customer Data**"). Company may internally use Customer Data to provide the Service to Customer and to improve the Service (during and after the term of this Agreement).
- 1.7 **Customer Equipment.** Customer is responsible for obtaining and maintaining any hardware, equipment, services, or other technology needed to connect to, access, or otherwise use the Service ("**Customer Equipment**"). Customer is responsible for the security of the Customer Equipment and for all uses of Customer Equipment.
- 1.8 **Feedback.** Customer may provide suggestions, comments or other feedback ("**Feedback**") to Company with respect to the Service. All Feedback is entirely voluntarily and shall not, absent a separate written agreement between the parties, create any confidentiality obligation for Company. Company shall own any Feedback provided by Customer and Company may freely use, disclose, reproduce, license, distribute, or exploit the Feedback during and following the Subscription Term without restriction.

## 2. **COMMERCIAL TERMS**

- 2.1 **Fees.** Customer shall pay Company the fees described in each Order. Unless otherwise set forth in an Order, Customer shall pay such fees not later than 60 days after receipt of Company's invoice therefor. All fees are based on subscriptions purchased and not actual usage. Payment obligations are not cancelable, and fees paid are non-refundable. Company reserves the right to change the applicable fees for the Service and to institute new charges and fees upon the expiration of the Subscription Term. Unpaid amounts are subject to a finance charge of 1.5% per month on any outstanding balance, or the maximum permitted by law, whichever is lower, plus all expenses of collection. Customer shall pay all taxes associated with the Service other than U.S. taxes based on Company's net income.
- 2.2 **Availability of Service.** Company shall provide the Services in accordance with the service level agreement attached hereto as Exhibit A.

- 2.3 **Support and Maintenance Services.** Company will use commercially reasonable efforts to provide Customer with all updates, upgrades, bug fixes, and error corrections to the Service that Company provides to its other customers.
- 2.4 **Term.** The term of this Agreement begins on the Effective Date (as defined below) and continues until the end of the last Subscription Term under the last Order. Unless otherwise set forth in an Order, the Subscription Term in an Order will automatically renew for an additional period equal to the original Subscription Term unless a party provides the other party with written notice of termination not less than 30 days prior to the expiration of the then-current Subscription Term.
- 2.5 **Effectiveness and Date.** This Agreement will become effective when all parties have signed it. Each party is signing this Agreement on the date stated opposite that party's signature. The date of this Agreement will be the date this Agreement is signed by the last party to sign it (as indicated by the date associated with that party's signature) (the "**Effective Date**"). If a party signs this Agreement but fails to date their signature, the date the other party receives the signing party's signature will be deemed to be the date the signing party signed this Agreement.
- 2.6 **Termination for Breach.** In addition to any other remedies it may have, a party may also terminate this Agreement on 30 days' notice if the other party materially breaches any of the terms or conditions of this Agreement and fails to cure such breach during such 30-day notice period. In the event Company terminates this Agreement as a result of Customer's uncured breach, Customer shall pay all fees through the entire Subscription Term. In the event Customer terminates this Agreement as a result of Company's uncured breach, Customer will pay in full for the Service up to and including the last day on which the Service is provided.
- 2.7 **Effect of Termination.** Upon termination of this Agreement, Company will immediately terminate Customer's access to the Service and either (1) Company shall be permitted to enter Customer's premises to retrieve any Company Equipment or (2) Customer shall promptly return Company Equipment at Company's cost and in accordance with Company's instructions. Obligations that are intended to survive the termination of this Agreement, including but not limited to Sections 2.7, 3, 4.2, 4.3, 4.4, 4.5, 4.6 and 5, shall survive the termination of this Agreement.
- 2.8 **Termination for Insolvency.** Either party may terminate this Agreement and any licenses granted hereunder, upon written notice if the other party: (a) becomes insolvent; (b) files has a petition filed against it, under Chapter 7 of the US bankruptcy code; or (c) ceases to carry on business in the ordinary course.
- 1.1 **Free Services.** The following applies to any use of the (i) Service that Company makes available to Customer without charging a fee ("**Free Services**") and (ii) services or functionality that Company makes available to Customer and that is not generally made available to Company customers and/or is designated as beta, pilot, preview, or similar designation ("**Beta Services**"). Unless otherwise set forth in an Order : (a) Free Services

and Beta Services offered at no charge will be subject to the Fees upon expiration of any free period term set forth in an applicable Order or if there is no term in an Order, upon 15 days' notice by Company; (b) free trials for new Customers have a 14-day term and Company's right to use customer name and logo under Section 5.8 will not be in effect during the free trial period; (c) Company reserves the right to discontinue or modify the provision of any Beta Services at any time with or without notice; (d) Section 2.2, 2.3, 4.1 and 4.2, to the extent they apply to Company, do not apply to Free Services and Beta Services; and (e) Company's liability for any losses or damages is subject to a cumulative and aggregate cap of \$5,000. . No Free Services shall be accepted, accessed, or utilized on behalf of Customer except by express written authorization of Customer, its Governing Board, agents, representatives, officers, consultants, employees, trustees, or volunteers.

### 3. CONFIDENTIALITY

- 3.1 **Definition.** "**Confidential Information**" means any information disclosed by a party ("**Disclosing Party**") to the other party ("**Receiving Party**"), whether before or after the date of this Agreement, that (1) is in written, graphic, machine readable or other tangible form and is marked "Confidential", "Proprietary" or in some other manner to indicate its confidential nature, (2) if not marked, Receiving Party should reasonably understand to be the confidential or trade secret information of Disclosing Party, or (3) is oral information disclosed by Disclosing Party to Receiving Party, provided that such information is designated as confidential at the time of disclosure and Disclosing Party reduces such information to writing within a reasonable time after its oral disclosure, and such writing is marked in a manner to indicate its confidential nature and delivered to Receiving Party.
- 3.2 **Obligations.** Receiving Party shall not use Confidential Information except to exercise its rights and perform its obligations under this Agreement. Receiving Party shall not disclose Confidential Information to any third party without the prior written approval of Disclosing Party. Receiving Party shall disclose Confidential Information internally only to those employees or independent contractors of Receiving Party who need to know Confidential Information in order for Receiving Party to exercise its rights and perform its obligations under this Agreement and who are bound by written confidentiality obligations at least as protective as this Agreement. Receiving Party shall take precautions to prevent disclosure or use of Confidential Information other than as authorized in this Agreement. Those precautions must be at least as effective as those taken by Receiving Party to protect its own Confidential Information or those that would be taken by a reasonable person in the position of Receiving Party, whichever are more effective. Receiving Party shall promptly notify Disclosing Party of any actual or suspected misuse or unauthorized disclosure of Disclosing Party's Confidential Information.
- 3.3 **Exceptions.** Receiving Party has no obligations under section 3.2 with respect to information that (1) was already public when Disclosing Party discloses it to Receiving

Party or becomes public (other than as a result of breach of this Agreement by Receiving Party) after Disclosing Party discloses it to Receiving Party, (2) when Disclosing Party discloses it to Receiving Party, is already in the possession of Receiving Party as the result of disclosure by a third party not then under an obligation to Disclosing Party to keep that information confidential, (3) after Disclosing Party discloses it to Receiving Party, is disclosed to Receiving Party by a third party not then under an obligation to Disclosing Party to keep that information confidential, or (4) was independently developed by Receiving Party without any use of or reference to Disclosing Party's Confidential Information.

- 3.4 **Compelled Disclosure.** If Receiving Party is required to disclose Confidential Information pursuant to the order or requirement of a court, administrative agency, or other governmental body, Receiving Party shall, to the extent allowed by law and prior to any such disclosure (1) provide prompt notice to Disclosing Party of such disclosure requirement and (2) cooperate with Disclosing Party to obtain a protective order or otherwise prevent public disclosure of such information. Receiving Party shall limit any required disclosure to the particular Confidential Information required to be disclosed.
- 3.5 **Return of Confidential Information.** Upon termination of this Agreement, Receiving Party shall promptly either deliver to Disclosing Party all of Disclosing Party's Confidential Information that Receiving Party has in its possession or control or at the request of Disclosing Party, destroy it. Notwithstanding the foregoing, (1) each party may retain Confidential Information that is contained in an automatic archived computer system backup; provided, however, that any such Confidential Information contained in such automatic archived computer system backup shall be subject to the terms and conditions of this Agreement and shall be accessible only to that party's IT professionals, and (2) nothing in this Agreement shall prohibit the party from retaining one copy of any of the Confidential Information with its legal counsel in a manner designed to ensure compliance with applicable law or legal process.
- 3.6 **Injunctive Relief.** Any breach of Receiving Party's obligations with respect to Confidential Information and intellectual property rights may cause substantial harm to Disclosing Party, which could not be remedied by payment of damages alone. Disclosing Party has the right to seek preliminary and permanent injunctive relief for such breach in any jurisdiction where damage may occur without a requirement to post a bond, in addition to all other remedies available to it for any such breach.
- 3.7 **Survival of Confidentiality Obligations.** Receiving Party shall comply with its obligations under this section 3 during the term of this Agreement and for a period of five (5) years thereafter, provided that for any Confidential Information that is a trade secret of Disclosing Party, such obligations shall continue in perpetuity for so long as such Confidential Information remains a trade secret.

#### 4. REPRESENTATIONS AND WARRANTIES; INDEMNIFICATION AND DISCLAIMERS



- 4.1 Representations and Warranties.** Each party states that it (i) has the power to enter into this Agreement, (ii) has all necessary rights, approval, permits and consents to enter into and perform its obligations under this Agreement, and that it will comply with all applicable laws in relation to its performance under this Agreement. Company warrants that (1) the Service will operate substantially in accordance with its documentation and (2) to the knowledge of Company, the Service when and as delivered or provided to Customer, is free of any code that is designed to disrupt, disable, harm, modify, delete, or otherwise impair the operation of the Service or any of Customer's software, computer systems, or networks. Company's sole and exclusive liability, and Customer's sole and exclusive remedy, for breach of the foregoing shall be Company's use of reasonable efforts to maintain the Service as described in this Agreement.
- 4.2 Company Indemnification.** Subject to the exceptions below, Company shall indemnify and defend and hold harmless Customer its Governing Board, agents, representatives, officers, consultants, employees, trustees, and volunteers ("Customer Indemnified Parties") against all third-party claims alleging that Customer's use of the Service as authorized hereunder infringes or misappropriates any United States patent, copyright, or trade secret (a "**Claim**"). Company shall have no obligation to indemnify Customer to the extent a Claim arises out of or is based on: (1) materials, equipment, software, or technology not supplied by Company, (2) Company's compliance with the written instructions provided by Customer, (3) modification of the Service by anyone other than Company, (4) combination of the Service with any materials, equipment, software, or technology where the alleged infringement would not have arisen in the absence of such combination, (5) Customer's alleged or actual breach of this Agreement, or (6) Customer's continuing the allegedly infringing, violating, or misappropriating activity after being notified or after being informed of modifications that would have avoided the alleged infringement. This section states Company's sole and exclusive liability to Customer, and Customer's sole and exclusive remedy for, claims of infringement, violation, or misappropriation of intellectual property rights.
- 4.3 Customer Indemnification.** Customer shall indemnify and defend Company and Company Individuals against all third-party claims alleging (1) that Company's use and exploitation of the Customer Data as authorized in this Agreement infringes, violates, or misappropriates any intellectual property rights or privacy rights or (2) any damages, costs, fines, judgments, losses, or liabilities arising out of Customer's use of the Service in violation of this Agreement (excluding any Claim for which Company has an obligation to indemnify).
- 4.4 Indemnification Procedure.** The indemnified party shall (1) promptly notify the indemnifying party of an applicable claim in writing, (2) give the indemnifying party sole control of the defense and settlement of the applicable claim, and (3) cooperate with the indemnifying party in the defense or settlement of a claim. An indemnified party may participate in the defense of a claim at its own expense.

**4.5 Disclaimer.** EXCEPT FOR THE EXPRESS WARRANTIES SET FORTH IN THIS AGREEMENT, THE SERVICE, COMPANY EQUIPMENT, AND DOCUMENTATION ARE PROVIDED “AS-IS,” “WHERE-IS,” AND “AS-AVAILABLE” WITH ALL FAULTS AND WITHOUT ANY WARRANTIES OF ANY KIND, AND COMPANY HEREBY EXPRESSLY DISCLAIMS ON BEHALF OF ITSELF AND ITS MEMBERS, STOCKHOLDERS, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS AND THIRD PARTY SUPPLIERS AND THEIR RESPECTIVE SUCCESSORS AND ASSIGNS (COLLECTIVELY, THE “**COMPANY PARTIES**”) ANY AND ALL OTHER WARRANTIES WHETHER, EXPRESS, IMPLIED OR STATUTORY, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, TITLE, FITNESS FOR A PARTICULAR USE OR PURPOSE, AND NON-INFRINGEMENT. NONE OF THE COMPANY PARTIES MAKES ANY REPRESENTATION OR WARRANTY THAT THE SERVICE OR COMPANY EQUIPMENT WILL MEET REQUIREMENTS, OR THAT THE SERVICE OR COMPANY EQUIPMENT WILL OPERATE WITHOUT INTERRUPTION, OR BE ERROR FREE; NOR DO THEY GUARANTEE ANY SPECIFIC RESULTS FROM USE. IN RECOGNITION OF THE ABOVE DISCLAIMER AND THE ALLOCATION OF RISK UNDER THIS AGREEMENT, CUSTOMER’S FINANCIAL OBLIGATIONS SHALL BE STRICTLY LIMITED TO THE COMPENSATION SET FORTH IN PARAGRAPH 3 (COMPENSATION). FURTHERMORE, NOTWITHSTANDING ANY OTHER PROVISION OF THIS AGREEMENT, AND CONSISTENT WITH THE LIMITATIONS ON WARRANTIES AND REMEDIES, AND NO EVENT SHALL CUSTOMER BE LIABLE WHETHER IN CONTRACT TORT OR OTHERWISE FOR ANY SPECIAL INDIRECT INCIDENTAL OR CONSEQUENTIAL DAMAGES INCLUDING LOST PROFITS OR REVENUE ARISING OUT OF OR RELATED TO THE SERVICES PERFORMED UNDER THIS AGREEMENT.

AS BETWEEN CUSTOMER AND THE COMPANY PARTIES, COMPANY IS SOLELY RESPONSIBLE FOR (AND HEREBY WAIVES, RELEASES AND DISCHARGES THE COMPANY PARTIES FROM ANY AND ALL LIABILITIES FOR) ANY AND ALL DAMAGES, LOSSES, AND INJURIES ARISING OUT OF, IN CONNECTION WITH, OR RESULTING FROM CUSTOMERS’ USE OF THE SERVICE OR COMPANY EQUIPMENT, INCLUDING ANY AND ALL DECISIONS MADE BY CUSTOMER ON THE BASIS OF SUCH USE.

CUSTOMER ACKNOWLEDGES THAT COMPANY DOES NOT CONTROL THE TRANSFER OF DATA OVER COMMUNICATIONS FACILITIES, INCLUDING THE INTERNET, AND THAT THE VOLT SERVICE MAY BE SUBJECT TO LIMITATIONS, DELAYS, AND OTHER PROBLEMS INHERENT IN THE USE OF SUCH COMMUNICATIONS FACILITIES. ACCORDINGLY, VOLT WILL NOT BE RESPONSIBLE FOR ANY DELAYS, DELIVERY FAILURES, OR OTHER DAMAGE RESULTING FROM SUCH PROBLEMS.

CUSTOMER ACKNOWLEDGES THAT THE SERVICE UTILIZES AI AND MACHINE LEARNING MODELS FOR SECURITY DETECTION AND RISK IDENTIFICATION. THE EFFECTIVENESS OF SUCH MODELS DEPENDS ON VARIOUS FACTORS, INCLUDING CUSTOMER-PROVIDED CONFIGURATIONS, CAMERA PLACEMENTS, AND EVOLVING THREAT PATTERNS.

AS A RESULT, COMPANY DOES NOT GUARANTEE THAT THE SERVICE WILL DETECT ALL SECURITY THREATS, UNAUTHORIZED INDIVIDUALS, WEAPONS, OR OTHER PROHIBITED ITEMS WITH 100% ACCURACY. COMPANY SHALL NOT BE LIABLE FOR ANY LOSSES,

DAMAGES, OR CLAIMS ARISING FROM FALSE POSITIVES, FALSE NEGATIVES, MISIDENTIFICATIONS, OR UNDETECTED THREATS WHILE USING THE SERVICE.

CUSTOMER EXPRESSLY ACKNOWLEDGES AND AGREES THE SERVICE AND COMPANY EQUIPMENT MAY RELY UPON THIRD-PARTY SOFTWARE AND HARDWARE FOR CERTAIN FUNCTIONS AND, EXCEPT AS SET FORTH EXPRESSLY HEREIN, COMPANY MAKES NO REPRESENTATION, WARRANTY, PROMISE, OR GUARANTEE TO RESELLER THAT SUCH SOFTWARE OR HARDWARE WILL BE ERROR FREE, ACCOMPLISH A SPECIFIED PURPOSE OR PERFORM IN ACCORDANCE WITH ANY PARTICULAR STANDARD, LEVEL OR METRIC AND COMPANY WILL NOT BE LIABLE TO RESELLER FOR ANY FAILURE THEREOF, IN PERFORMANCE OF THE SECURITY DETECTION. HOWEVER COMPANY IS STILL LIABLE FOR ANY 3RD PARTY BREACH OF DATA SECURITY OR INFORMATION THAT IS OTHERWISE PROTECTED IN THIS AGREEMENT OR OTHER AGREEMENTS BETWEEN THE PARTIES SUCH AS CA-NDPA

- 4.6 Limitation of Liability.** Except for breach of Section 2, in no event will Company be liable to Customer for any consequential damages or damages related to loss of data, loss of system availability, Service failure or lack of Service performance, loss of computer run time, or lost profits or revenue. The foregoing limitations will survive and apply notwithstanding any failure of the essential purpose of any limited remedy provided in this Agreement. Company is not responsible for any actions taken by Customer, its staff, or law enforcement agencies in response to alerts or data generated by the Service. Customer acknowledges that Company does not control or dictate the interpretation of alerts, nor the decisions made by Customer based on the Service's outputs. Company's maximum liability for any claim arising from or related to the Service shall not exceed the total fees paid by Customer in the 12 months preceding the claim.

## **5. MISCELLANEOUS**

- 5.1 Governing Law.** California law governs all adversarial proceedings arising out of this Agreement.
- 5.2 Venue.** California law governs all adversarial proceedings arising out of this Agreement. Customer hereby consents to the exclusive jurisdiction and venue of the courts of the State of California or, if appropriate, the United States District Court for the applicable district in California for any residual claims In the event of arbitration or litigation arising out of or relating to this Agreement, or the Service provided under this Agreement, the prevailing party shall be entitled to recover attorney's fees, and all other related and reasonable expenses incurred in such arbitration or litigation, from the other party.
- 5.3 Severability.** The parties acknowledge that if a dispute between the parties arises out of this Agreement or the subject matter of this Agreement, they would want the court to interpret this Agreement as follows: (1) with respect to any provision that it holds to be unenforceable, by modifying that provision to the minimum extent necessary to make it enforceable or, if that modification is not permitted by law, by disregarding that provision; (2) if an unenforceable provision is modified or disregarded in accordance

with this section, by holding that the rest of the Agreement will remain in effect as written; (3) by holding that any unenforceable provision will remain as written in any circumstances other than those in which the provision is held to be unenforceable; and (4) if modifying or disregarding the unenforceable provision would result in failure of an essential purpose of this Agreement, by holding the entire Agreement unenforceable.

- 5.4 **California Student Data Privacy Compliance.** To the extent the Services are provided to K–12 schools in California, Provider shall comply with all applicable state laws governing student data privacy, including but not limited to the California Consumer Privacy Act as amended by the California Privacy Rights Act (“CCPA/CPRA”), the Student Online Personal Information Protection Act (“SOPIPA,” Cal. Bus. & Prof. Code § 22584), and relevant sections of the California Education Code. Provider affirms that it does not and will not sell, share, or disclose student personal information for any purpose other than those explicitly authorized by the Customer in connection with the educational or school safety purpose of the Services. Provider further agrees not to use such data for targeted advertising, behavioral profiling, or unrelated commercial purposes, and shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect student data from unauthorized access, destruction, use, modification, or disclosure. Provider will support the Customer’s compliance with applicable California laws by facilitating access to, correction of, or deletion of student data upon request, and will provide prompt breach notification in accordance with California Civil Code § 1798.29.
- 5.5 **Waiver.** No waiver of satisfaction of a condition or nonperformance of an obligation under this Agreement will be effective unless it is in writing and signed by the party granting the waiver.
- 5.6 **Assignment.** Except with the prior written approval of Company, Customer shall not transfer, including by merger (whether that party is the surviving or disappearing entity), consolidation, dissolution, or operation of law, (1) any discretion, right, or license granted under this Agreement, (2) any right to satisfy a condition under this Agreement, (3) any remedy under this Agreement, or (4) any obligation imposed under this Agreement. Any purported transfer in violation of this section will be void.
- 5.7 **Amendment.** No modification of this Agreement will be effective unless it is in writing and signed by the parties.
- 5.8 **Notices.** For a notice of other communication under this Agreement to be valid, it must be in writing and delivered (1) by hand, (2) by a national transportation company (with all fees prepaid), (3) by registered or certified mail, return receipt requested and postage prepaid, or (4) by email, when directed to the email address below. A valid notice or other communication under this Agreement via the methods (1) through (3) above will be effective when received by the party to which it is addressed and if via email, when receipt is confirmed by a non-automated response. If the party to which it is addressed rejects or otherwise refuses to accept it, or if it cannot be delivered because of a change

in address for which no notice was given, the notice or communication will be deemed received upon that rejection, refusal, or inability to deliver. Notices or other communications to a party must be addressed using the information specified below for that party or any other information specified by that party in a notice under this section.

**Company Notice:**


Attn: VOLT Legal  
Egor Olteanu  
4600 East-West Hwy  
Bethesda, MD 20814  
Email: [legal@volt.ai](mailto:legal@volt.ai)

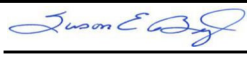
**Customer Notice:**

Attn:  
  
  
  
Email:

5.9 **Publicity.** Neither party shall, except as otherwise required by Applicable Law or stock exchange requirements, issue or release any announcement, statement, press release or other publicity or marketing materials relating to this Agreement or otherwise use the other party’s marks or logos without the prior written consent of the other party; provided, however, Company may include Customer’s name and logo in its lists of Company customers, its public website and other promotional material, in each case in accordance with any Customer brand guidelines to the extent available to Company. Company agrees to cease such uses of Customer’s name and logo within 30 days following Customer’s request submitted at [info@volt.ai](mailto:info@volt.ai).

5.10 **Entire Agreement.** This Agreement constitutes the entire agreement between the parties relating to its subject matter, and supersedes all prior or contemporaneous discussions, or presentations and proposals, written or oral relating to such subject matter.

	<b>VOLT, INC.</b>
Date: <u>6/5/2025</u> , 2025	DocuSigned by: <u>By: </u> 92250C55CA044E2...
	Name: <u>Julia Fletcher</u>
	Title: <u>VP of Finance</u>

	<b>Oakland Unified School District</b>
Date: <u>6/18/2025</u> , 2025	By: <u></u>
	Name: <u>Susan Beltz</u>
	Title: <u>Chief Technology Officer</u>



## Exhibit A

### Service Level Agreement

**1. Up-Time and Reliability:** Company will use reasonable commercial efforts with the intent that Services will be available and operational to Customer for 99% of all Scheduled Availability Time. "Scheduled Availability Time" shall be defined as twenty-four (24) hours a day, seven (7) days a week, excluding: (i) scheduled maintenance downtime; (ii) maintenance downtime for specific critical Service issues; and (iii) any downtime due to defects caused by Customer, one of its vendors, third party connections, utilities, or caused by other forces beyond the control of Company (such as internet outages or outages with respect to Customer's network or internet access) and (iv) individual camera downtime or individual stream interruption. Company shall use reasonable efforts to provide advance notice in writing or by email of any scheduled service disruption.

**2. Maintenance:** Company will make available to Customer as part of the Services, all generally available enhancements, updates and bug fixes to the Services.

**3. Customer Responsibility:** In addition to other responsibilities contained herein, Customer will be responsible for ongoing accuracy of the information supplied to Company from Customer pertaining to Customer's billing and finance department.

**4. Support:** Company is available to receive product support inquiries via email or the Company website 24 hours per day. Company Standard Support Hours are 9:00 to 17:00 Eastern Time Monday through Friday for technical information, technical advice and technical consultation regarding Customer's use of the Services.

**5. Customer Support List:** Customer shall provide to Company, and keep current, a list of designated contacts and contact information (the "Support List") for Company to contact for support services. Such Support List shall include (i) the first person to contact for the answer or assistance desired, and (ii) the persons in successively more responsible or qualified positions to provide the answer or assistance desired.

**6. Classification of Problems:** Company shall classify each problem encountered by Customer according to the following definitions and will use reasonable commercial efforts to address the problem in accordance with such classification according to the table below.

7. SEVERITY LEVELS AND RESPONSE TIMES

Priority code	Priority description	Action required	Expected response times
P1	<b>Mission Critical.</b> Data collection services and data reporting services are down, causing critical impact to business operations; no workaround available.	Escalation in accordance with provisions “Escalation procedures” section below.	Company will provide a status update by telephone and/or e-mail. Company’s goal for resolution of P1 issues is within two (2) calendar days of Customer’s receipt of issue notification.
P2	<b>High.</b> Data collection services and data reporting services are significantly degraded and/or impacting significant aspects of business operations.	Escalation in accordance with provisions “Escalation procedures” section below.	Company will provide a status update by telephone, e-mail, or via automated notification within the reporting interface of the Measurement Services as mutually agreed upon by the Parties, as warranted until (i) the problem is resolved, (ii) an acceptable workaround is found or (iii) the problem is determined to be outside of Company’s ability to control.
Priority code	Contact type	Name of Volt.ai contact / Role	Contact Email address
P1	<b>Primary</b>	Key Tech Staffer/ First Available	help@volt.ai
	Secondary	Customer Success Team	support@volt.ai
P2	<b>Primary</b>	All Staff / First Available	help@volt.ai
	Secondary	Customer Success Team	support@volt.ai





**Volt Inc**  
**4600 East-West Hwy, Suite 620**  
**Bethesda, MD 20814**

**DATE**  
03/05/2025  
**SALES ORDER NO.**  
2025-00012

**Customer Name** Oakland Unified School District

**Quote prepared by** Colin Quirk

**Contact** Susan Beltz, Chief Technology Officer  
**Address** 1011 Union Street, Oakland, CA 94607  
**Phone** 510.879.8873  
**Email** susan.beltz@ousd.org

**Phone** 770.713.2934  
**Email** colin@volt.ai

		Unit	Streams	Price	OUSD Price
<b>VOLT AI Video Intelligence Professional</b> <ul style="list-style-type: none"><li>- Real-time AI-powered platform that analyzes all security streams 24/7</li><li>- Interactive digital twin of your facilities</li><li>- Continuously evolving cutting edge Machine Learning models trained to detect a wide range of scenarios</li><li>- Human-in-the-loop validation to minimize false positives</li><li>- Company-wide access with tiered access levels</li><li>- Mobile notifications</li><li>- Optional 911 auto-dialer</li></ul>		2 Months	47	\$3,008	
	In-Person Implementation <ul style="list-style-type: none"><li>-3D Mapping of Floor Plans and Facility</li><li>- Installation of Hardware on-site</li><li>- Verify server connection and ensure cameras are online</li><li>- Establish monitoring rules and escalation policy</li><li>- Live, in-person functional test of streams &amp; policies</li><li>- Additional Virtual Training for Admins</li></ul> All necessary 2U/1U Edge Devices (Installed Servers)	one-time	47	<del>\$301</del> Included	
	Premium Support <ul style="list-style-type: none"><li>- Dedicated, technical support representative</li><li>- Ongoing stream set-up support and offline monitoring</li><li>- Ongoing stream detection tests</li><li>- Feature request prioritization</li></ul>	2 Months	47	<del>\$564</del> Included	

**Subscription Term**

1/20/2025-3/16/2025

**Payment Terms** Net 30

Subject to Signed Volt AI MSA

Customer Responsible for all applicable Sales, Use, or VAT taxes.

<b>Total</b>	\$3,008.00
<b>One-Time Total</b>	\$0.00
<b>2 Month Total</b>	\$3,008.00
<b>Number of Months</b>	2
<b>Invoice Total</b>	\$ 3,008.00

Oakland Unified School District

VOLT AI

Signature \_\_\_\_\_  
Print \_\_\_\_\_  
Date \_\_\_\_\_

Signature \_\_\_\_\_  
Print Julia Fletcher, Head of Finance  
Date \_\_\_\_\_

**Volt Inc****4600 East-West Hwy, Suite 620****Bethesda, MD 20814****DATE**

03/05/2025

**SALES ORDER NO.**

2025-00013

**Customer Name** Oakland Unified School District**Quote prepared by**

Colin Quirk

**Contact** Susan Beltz, Chief Technology Officer**Address** 1011 Union Street, Oakland, CA 94607**Phone** 770.713.2934**Phone** 510.879.8873**Email** susan.beltz@ousd.org**Email** colin@volt.ai

		Unit	Streams	Price
<b>VOLT AI Video Intelligence Professional</b> <ul style="list-style-type: none"><li>- Real-time AI-powered platform that analyzes all security streams 24/7</li><li>- Interactive digital twin of your facilities</li><li>- Continuously evolving cutting edge Machine Learning models trained to detect a wide range of scenarios</li><li>- Human-in-the-loop validation to minimize false positives</li><li>- Company-wide access with tiered access levels</li><li>- Mobile notifications</li><li>- Optional 911 auto-dialer</li></ul>		6 Months	128	\$24,576.00
	In-Person Implementation <ul style="list-style-type: none"><li>-3D Mapping of Floor Plans and Facility</li><li>- Installation of Hardware on-site</li><li>- Verify server connection and ensure cameras are online</li><li>- Establish monitoring rules and escalation policy</li><li>- Live, in-person functional test of streams &amp; policies</li><li>- Additional Virtual Training for Admins</li></ul> All necessary 2U/1U Edge Devices (Installed Servers)	one-time	128	\$2,457 Included
	Premium Support <ul style="list-style-type: none"><li>- Dedicated, technical support representative</li><li>- Ongoing stream set-up support and offline monitoring</li><li>- Ongoing stream detection tests</li><li>- Feature request prioritization</li></ul>	6 Months	128	\$4,608 Included

**Total** \$24,576**Subscription Term: 3/17/2025-9/17/2025****One-Time Total** \$2,457 Included**Payment Terms: Net 30****Number of Months** 6

Subject to Signed Volt AI MSA

**6 Month Invoice Total** \$ **24,576.00**

Customer Responsible for all applicable Sales, Use, or VAT taxes.

Oakland Unified School District

VOLT AI

Signature \_\_\_\_\_  
Print \_\_\_\_\_  
Date \_\_\_\_\_

Signature \_\_\_\_\_  
Print Julia Fletcher, Head of Finance  
Date \_\_\_\_\_

# **STANDARD STUDENT DATA PRIVACY AGREEMENT**

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

**Oakland Unified School District**

**and**

**Volt, Inc.**

June 3, 2025

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 Street Oakland, CA 94607  
(the “**Local Education Agency**” or “**LEA**”) and

Volt, Inc. , located at 4600 East West Hwy Ste. 620 Bethesda, MD 20814  
(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: Susan Beltz Title: Chief Technology Officer

Address: 1011 Union Street Oakland, CA 94607

Phone: 510-879-8873 Email: susan.beltz@ousd.org

The designated representative for the Provider for this DPA is:

Name: Dmitry Sokolowski Title: Founder

Address: 4600 East West Hwy Ste. 620 Bethesda, MD 20814

Phone: 240-476-7681 Email: dmitry@volt.ai

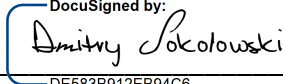
**IN WITNESS WHEREOF**, LEA and Provider execute this DPA as of the Effective Date.

**LEA:** **Oakland Unified School District**

By:  Date: 6/18/2025

Printed Name: Susan Beltz Title/Position: Chief Technology Officer

**PROVIDER:** **Volt, Inc.**

By:  Date: June 3, 2025

Printed Name: Dmitry Sokolowski Title/Position: CTO & Co-Founder

## **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**

Volt provides a real-time video intelligence platform that integrates with a school's existing security camera infrastructure to enhance safety, situational awareness, and emergency response. The platform uses AI-powered analytics to detect and track people, objects, and behaviors across a school campus on a digital map interface accessible only by authorized staff.

Volt's services include:

AI-based detection of behavioral anomalies (e.g., loitering, fights, perimeter breaches)

Dynamic tracking of individuals across camera zones without identity resolution

3D mapping and visualization of movement across school grounds

Secure, role-based access for school administrators and safety personnel

No student logins or accounts are used. No personally identifiable student information is collected, stored, or processed. All system users are school staff or authorized personnel. Any detected individuals are processed as anonymous figures and are not linked to student records.

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

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

Category of Data / Data Elements	ALL DPA- COVERED APPS						
Other enrollment information							
<i>If 'Other' checked, please specify below checked box:</i>							
<b>Parent/Guardian Contact Information</b>							
Address							
Email							
Phone							
<b>Parent/Guardian ID</b>							
Parent ID number (created to link parents to students)							
<b>Parent/Guardian Name</b>							
First and/or last							
<b>Schedule</b>							
Student scheduled courses							
Teacher names							
<b>Special Indicator</b>							
English language learner information							
Low-income status							
Medical alerts/health data							
Student disability information							
Specialized education Services (IEP or 504)							
Living situations (homeless/foster care)							
Other indicator information							

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



Category of Data / Data Elements	ALL DPA- COVERED APPS						
<b>Student Survey Responses</b>							
Student responses to surveys or questionnaires							
<b>Student Work</b>							
Student generated content; writing, pictures, etc.							
Other student work data							
<i>If 'Other' checked, please specify below checked box:</i>							
<b>Transcript</b>							
Student course grades							
Student course data							
Student course grades/performance scores							
Other transcript data							
<i>If 'Other' checked, please specify below checked box:</i>							
<b>Transportation</b>							
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>							
<b>Other</b>							
Other data collected							
<i>If 'Other' checked, please list each additional data element used, stored, or collected by your application below checked box:</i>							
<b>None</b>							
No student data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	X						

## **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

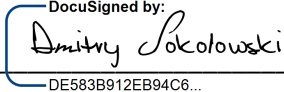
**EXHIBIT “E”**  
**GENERAL OFFER OF PRIVACY TERMS**

**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 June 3, 2025 , 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:

**PROVIDER:** Volt, Inc.

BY:  DE583B912EB94C6... Date: June 3, 2025

Printed Name: Dmitry Sokolowski Title/Position: CTO & Co-Founder

**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:** \_\_\_\_\_

BY: \_\_\_\_\_ Date: \_\_\_\_\_

Printed Name: \_\_\_\_\_ Title/Position: \_\_\_\_\_

SCHOOL DISTRICT NAME: \_\_\_\_\_

DESIGNATED REPRESENTATIVE OF LEA:

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Address: \_\_\_\_\_

Telephone Number: \_\_\_\_\_

Email: \_\_\_\_\_

**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

	<b>MAINTAINING ORGANIZATION/GROUP</b>	<b>FRAMEWORK(S)</b>
X	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)
X	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)

## 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 Street Oakland, CA 94607  
(the "**Local Education Agency**" or "**LEA**") and  
**Volt, Inc.**, located at 4600 East West Hwy Ste. 620 Bethesda, MD 20814  
(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:  DATE: 6/18/2025

Printed Name Susan Beltz Title/Position Chief Technology Officer

Provider: Volt, Inc.

BY:  DATE: June 3, 2025

Printed Name Dmitry Sokolowski Title/Position CTO & Co-Founder

## 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>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Adaptive Learning/Assessment Platforms	<i>Adjusts the difficulty level and content of learning materials based on the student's performance and learning pace</i>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Natural Language Processing (NLP)	<i>Analyze and understand students' written or spoken responses, providing feedback or assistance in language learning tasks.</i>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
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>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Virtual Assistants (i.e. Alexa, Siri, Merlyn Mind)	<i>Provide automated and personalized support by handling tasks, answering questions, and managing workflows.</i>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
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>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Data Analytics and Predictive Modeling	<i>Analyze historical data and identify patterns to forecast future trends and inform strategic decision-making.</i>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
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>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
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>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Recommender Systems/Filtering (i.e. KNN, TF-IDF)	<i>Analyze user preferences and behavior to suggest personalized content, products, or services</i>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
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>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
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>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Speech Recognition (i.e. DNNs, Wav2Vec)	<i>Convert spoken language into text by accurately identifying and processing the acoustic signals of human speech.</i>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

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.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
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.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
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.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Other Types of AI Used	Specify other types of AI here:	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Purpose of AI Use	Description	Optional	Required
Personalized learning	Customized learning to match a students' strengths, weaknesses, and learning styles.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Enhanced Teaching and Learning	Assist teachers in delivering more effective instruction and help students grasp difficult concepts more easily.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Automated Grading and Feedback	Automate the grading for assignments, quizzes, and exams; provides immediate feedback to students.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Identifying Learning Gaps	Analyze student performance data to identify areas where students are struggling and provide targeted interventions to address learning gaps.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Supporting Special Education	Additional support and accommodations for students with special needs, including personalized learning plans and assistive technologies	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Promoting Engagement and Motivation	Gamification elements and interactive learning experiences; increase student engagement and motivation	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Administrative Support	Assist with administrative tasks such as scheduling, grading, and managing educational resources	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Parental Engagement	Provide parents with insights into their student's academic progress, for communication and collaboration between parents, students, and teachers	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Other Purpose(s) for AI Use	Specify other purpose(s) for AI here: Improve safety of students and faculty, helping to identify medical emergencies, fighting, weapons on campus and other safety and security risks.	<input type="checkbox"/>	<input checked="" type="checkbox"/>

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

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