SERVICES AGREEMENT

This Services Agreement and any ordering document executed by the Parties or online registration request that is accepted by Playlab referencing this Services Agreement (such ordering document, a "**Statement of Work**" and the Statement of Work together with this Services Agreement, the "**Agreement**") collectively constitute a binding agreement between Playlab Education Inc., ("**Playlab**"), and Ector County Independent School District ("**Customer**"). Customer and Playlab may be referred to individually as a "**Party**" and collectively, the "**Parties**." The "**Effective Date**" of this Agreement will be the date both Parties have signed the Agreement.

PLEASE READ THIS AGREEMENT CAREFULLY. THIS AGREEMENT GOVERNS YOUR USE OF THE SERVICE. BY SIGNING THIS AGREEMENT, YOU REPRESENT THAT (1) YOU HAVE READ, UNDERSTAND, AND AGREE TO BE BOUND BY THIS AGREEMENT, (2) YOU ARE OF LEGAL AGE TO FORM A BINDING CONTRACT WITH PLAYLAB, AND (3) YOU HAVE THE AUTHORITY TO ENTER INTO THE AGREEMENT AND TO BIND THE CUSTOMER TO THE AGREEMENT. IF YOU DO NOT AGREE TO BE BOUND BY THIS AGREEMENT, YOU MAY NOT ACCESS OR USE THE PLAYLAB SERVICE.

Definitions

1. Definitions.

"**Aggregated and De-identified Data**" means aggregated, anonymized or deidentified data or information of similar form, derived from Customer Content that is created by or on behalf of Playlab. For clarity, such data excludes personally identifiable information of Customer or any Authorized User.

"**Authorized Account Administrators**" means Authorized Users with administrative permissions, which may include restricting certain features and functionality and restricting access of Customer's Organization to certain users.

"**Authorized User**" means any individual authorized by Customer to access and use the Service, including employees, teachers, aides, other school personnel and students.

"**Customer Content**" means all data, images, and content submitted, transmitted, or made available by or on behalf of Customer and its Authorized Users into the Service and all Output.

"**Output**" means output generated through use of the Service (such as any App) based on Customer Content.

"**Platform**" means Playlab's proprietary software-as-a-service platform designed to allow Authorized Users to (a) develop educational applications and tools leveraging Playlab's AI Features (collectively, "**Apps**"), and (b) access, use, and modify Apps designed by other users in such Authorized User's Organization and Apps that are designated as publicly available (each, a "**Community App**").

"**Service**" means any professional services indicated on the Statement of work (including any training or onboarding sessions), the Platform, and the hosting and provision of the Platform.

"**Organization**" means the designated organization on the Service solely for Customer and Authorized Users. Organizations may include Apps designed by Authorized Users that are solely accessible and usable by other Authorized Users of the same Organization.

2. Playlab Responsibilities

2.1. Provision of the Service. Subject to the terms and conditions of this Agreement and during the Term, Playlab will make the Service available to Customer for use by Authorized Users solely for educational

purposes. Playlab may update the functionality, user interfaces, and usability from time to time in its sole discretion as part of its ongoing mission to improve the Service.

2.2. Support. Subject to the terms of this Agreement, Playlab shall provide Customer with Playlab's standard support services to assist Customer in its use of the Service and will use commercially reasonable efforts to maintain the availability of the Service.

2.3. Compliance with Laws. Playlab will comply with all laws applicable to Playlab's provisioning of the Service.

3. Access to and Use of the Service

3.1. Accounts. As part of the set-up process, one or more accounts on the Platform may be created and/or provisioned for Customer and/or its Authorized Users (each, an "**Account**"). Customer represents and warrants that all Account registration information provided by or on behalf of Customer is truthful and accurate, and Customer will maintain the accuracy of such information. Accounts may only be used by one Authorized User, and Customer is responsible for maintaining the confidentiality of all Account login information. Customer is fully responsible for: (a) designating which Authorized Users are Authorized Account Administrators; (b) determining which individuals may access Customer's Organization (and terminating such access as appropriate); and (c) all other activities that occur under Customer's and its Authorized Users' Accounts. If any Authorized User is no longer a student, employee, or contractor of Customer, Customer will notify Playlab to terminate such Authorized User's Account.

3.2. Eligibility. Playlab reserves the right to implement eligibility requirements for Authorized Users if required by law and will provide notice of any changes to the eligibility requirements.

3.3. Customer Responsibilities. Customer will: (a) obtain any licenses, permissions, and consents required for Authorized Users to access and use the Customer Content in connection with the Service, including with respect to the license grants in Section 7.1; (b) be fully responsible for Authorized Users' compliance with this Agreement; (c) be responsible for the accuracy, completeness, appropriateness, and legality of Customer Content; (d) use commercially reasonable efforts to prevent unauthorized access to or use of the Service, and promptly notify Playlab of any such unauthorized access or use or any suspected unauthorized access or use; and (e) use the Service only in accordance and compliance with all applicable laws and government regulations. Playlab will not be liable for any loss or damage arising from any unauthorized use of the Accounts or Customer's failure to comply with the foregoing requirements. Customer and its Authorized Users will have access to the Customer Content and will be responsible for all changes to and/or deletions of Customer Content and the security of all passwords and other usernames and passwords required in order the access the Service. Customer is encouraged to make its own back-ups of the Customer Content. Any act or omission by an Authorized User that, if done by Customer, would constitute a breach of this Agreement, shall be deemed a breach of this Agreement by Customer.

3.4. System Requirements. A high-speed Internet connection is required for proper use of the Platform. Customer is responsible for procuring and maintaining the network connections that connect its network to the Platform, including, but not limited to, browser software that supports protocols used by Playlab, and following procedures for accessing services that support such protocols. Playlab assumes no responsibility for the reliability or performance of any connections as described in this Section.

3.5. Usage Restrictions. Customer will not, and will not permit any Authorized User or third party to directly or indirectly: (a) except as expressly permitted in this Agreement, make the Service available to, or use the Service for the benefit of, anyone other than Customer and the Authorized Users; (b) upload, post, transmit, or otherwise make available to the Service any content that (i) is unlawful or tortious, (ii) infringes, misappropriates, or otherwise violates any intellectual property, privacy, publicity, or other proprietary rights of any person, (iii) is harmful to the Service (including, without limitation, "Trojan horses," "viruses," "worms," "time bombs," "time locks," "devices," "traps," "access codes," or "drop dead" or "trap door" devices); (c) sublicense, rent, resell, time share, or similarly exploit the Service; (d) upload, post, transmit, or otherwise make available any content or information designed to interrupt, interfere with, destroy or limit the functionality of any computer software or hardware or telecommunications

equipment; (e) reverse engineer, modify, adapt, or hack the Service, or otherwise attempt to gain unauthorized access to the Service or its related systems or networks; (f) except as expressly permitted in this Agreement, copy or modify the Service, or create any derivative works from either of the foregoing; (g) interfere with, disrupt, or create an undue burden on (or violate the regulations, policies, or procedures of) any servers or networks connected to the Service; (h) access the Service to build a competitive product or service; or (g) otherwise use the Service except as expressly permitted under this Agreement.

3.6. Third-Party Services; AI Features.

3.6.1. Customer acknowledges and agrees that the Service may include content and/or services provided by third parties ("**Third-Party Content and Services**"), including other users, that are not under the control of Playlab. Playlab does not approve or endorse, or make any representations or warranties with respect to such Third-Party Content and Services, and Customer and its Authorized Users use such Third-Party Content and Services at their own risk. When interacting with any third parties via the Service, including the Platform and any training sessions, Customer and its Authorized Users assume the risks of such interactions, and Customer agrees that it is solely responsible for its and its Authorized Users' interactions with other third parties via the Services; provided, however, that Playlab reserves the right, but has no obligation, to intercede in any disputes that may arise. Customer agrees that Playlab will not be responsible for any liability incurred as the result of the Customers or its Authorized Users' interactions with third parties via the Services whether online or offline. Certain Third-Party Content and Services, such as links to Playlab's social media page on other platforms, may also be subject to additional terms and conditions (including privacy policies). If Customer or its Authorized Users engages with such Third-Party Content and Services, Customer and its Authorized Users are responsible for reviewing all applicable terms and policies and making whatever investigation is necessary and appropriate before proceeding with any transaction or interaction.

3.6.2. Customer acknowledges and agrees that certain features of the Platform utilize artificial intelligence technology, including large language models ("***AI Features***"). Customer acknowledges and agrees that when using these AI Features, Customer Content will be transmitted to third-party service providers. Customer acknowledges it is solely responsible for its and its Authorized Users' use of all AI Features. As between the Parties, any Output is considered Customer Content. Customer accepts that, as AI Features utilize artificial intelligence technology, such features may provide Output that is inaccurate or inappropriate as a response to the input provided. Due to the nature of machine learning, Output may not be unique across users and the Platform may generate the same or similar output for Playlab or a third party. Other Playlab customers may also provide similar customer prompts as inputs to the Platform and receive generated content that is similar or identical to Output. Customer has no right, title or interest in or to generated content provided to third parties, regardless of the level or degree of similarity. Customer is responsible for evaluating the accuracy and suitability of Output as appropriate for Customer's use case, assessing any potential biases, and subjecting Output to Customer's standard quality control procedures within its business, including by using human review of Output. Customer agrees that Playlab shall have no responsibility or liability arising from the provision of inaccurate or inappropriate Output or any decisions made in reliance on such Output, and that such decisions are made at the Customer's own risk.

3.6.3. Customer acknowledges and agrees that the use of Third-Party Content and Services, including the transmission of certain Customer Content to the applicable third-party service providers (such as the providers of AI Features) is an integral and necessary part of Playlab's delivery of the Service. Customer agrees that Playlab shall have no responsibility or liability arising from any use, storage, data breach, or deletion of such Customer Content by the providers of the Third-Party Content and Services. Playlab cannot guarantee the continued availability of Third-Party Content and Services and may temporarily or permanently cease providing, without entitling Customer to refund, credit, or compensation, any particular Third-Party Content and Services if the applicable provider suspends, modifies, or alters such services.

3.7. Community App. Customer acknowledges and agrees that Customer may access, use, and modify Community Apps on the Platform designed by other users of the Platform. Such Community Apps may be

subject to additional policies of Playlab, which shall be presented by Playlab at the time of use. Without limiting Section 10.3, Customer agrees, and shall cause its Authorized Users to agree, that Playlab shall have no responsibility or liability arising from use of the Community Apps and the provision of inaccurate or inappropriate Output via Community Apps or any decisions made in reliance on any Community App is at Customer's own risk. Further, third parties may access, use, and modify Apps that Customer or Customer's Authorized Users choose to make a Community App. Customer acknowledges that all such Community Apps, whether made using Customer Content or not, will be publicly available via the Platform for third parties, including other users of the Platform, to access and use in accordance with Playlab's agreement with such users during and after the Term. Accordingly, Playlab encourages Customer to inform its Authorized Users of any applicable Customer policies or restrictions with respect to using any Customer Content (e.g. confidentiality policies, third-party license restrictions, policies with respect to student data, etc.) when creating or using Community Apps. Customer is solely responsible for enforcing any such policies or restrictions with respect to the use of the Platform.

3.8. Embedding Feature. As a paying customer, Customer may have access to certain features and functionality that enable Customer's Authorized Users to embed certain Apps on a platform owned by, or operated by, Customer (such feature, an "**Embedding Feature**" and such platform, a "**Customer Website**"). Subject to the terms and conditions of this Agreement, Playlab hereby grants Customer and its Authorized Users a nonexclusive, nontransferable, nonsublicensable license, during the Term, to: (i) embed and incorporate Apps that Customer has permissions to access into Customer Websites; and (ii) display the public facing portions of such Apps to end users of the Customer Website solely as embedded and incorporated via the Embedding Feature and solely pursuant to any policies presented with the Embedding Feature (as may be updated from time to time).

4. Integrations with Customer Environments. If supported by Playlab, the Service may integrate with third-party services (e.g., Clever or OpenID) for which Customer has independently contracted ("**Customer Environment**"). If Customer elects to integrate its Playlab account for which it is responsible hereunder with one or more Customer Environments supported by Playlab, it shall ensure that it has all required permissions and authorizations to share such information with Playlab for such limited purpose. Any integration with a Customer Environment ("**Integration**") depends on the continuing availability of, and access to such Customer Environment and/or any content or interfaces made available through such Customer Environment. If for any reason Playlab cannot access or use the applicable Customer Environment or the required data or information interfaces, Playlab may not be able to provide all of the functions of its Service. No refund or credit will be provided for unavailability of any Customer Environment. Unless otherwise specified in this Agreement, all content or data accessed through Customer Environment integrated hereunder will be considered to be Customer Content for purposes of this Agreement. Where Customer elects to create an Integration for use with Customer's Student Information System (SIS), it agrees to apply minimum technical requirements and comply with the acceptable use parameters (e.g., requirements for usernames, passwords, password reset, end point maintenance, and testing environments).

5. Fees.

5.1. Fees. The Parties agree that all fees set forth on the applicable Statement of Work ("**Fees**"), which is attached hereto and incorporated herein by reference as Exhibit "B," shall be paid by Permian Strategic Partnership Inc. ("PSP") in accordance with any payment terms set forth in the Statement of Work. PSP and Playlab have agreed to the payment terms and conditions for the Services in a separate, written agreement. If Customer exceeds the usage limitations as set forth in the Statement of work, Playlab reserves the right to invoice PSP for such overages. All Fees are quoted in United States Dollars and, except as set forth otherwise in this Agreement, are non-refundable. Unless otherwise expressly specified in the applicable Statement of work, PSP will pay all invoices within thirty (30) days from the date of invoice. PSP will be responsible for any costs resulting from collection by Playlab of any such overdue balance, including, without limitation, reasonable attorneys' fees and court costs.

6. Playlab Proprietary Rights

6.1. Playlab Property. Subject to Customer's rights in the Customer Content, Playlab retains all rights, title, and interest in and to the Service, including all modifications, derivative works made by Playlab, upgrades, and updates thereto, and all related intellectual property rights therein. No rights are granted by Playlab hereunder other than as expressly set forth herein. If Customer or any Authorized User provides Playlab with any feedback or suggestions regarding the Service, then Customer grants Playlab an unlimited, irrevocable, perpetual, sublicensable, royalty-free license to use any such feedback or suggestions for any purpose without any obligation or compensation to Customer or any Authorized User.

6.2. Performance Data. Playlab may create, generate, and use general performance and usage data in connection with Customer's use of the Service (such as technical logs, account and login data, and processed volumes) ("**Performance Data**"). Playlab retains all right, title, and interest, including all intellectual property rights, in and to the Performance Data and may freely use such Performance Data for any lawful purpose, including for training, improving, and analyzing the Service. For purposes of this Agreement, Performance Data does not contain any and does not constitute Personal Data (as defined in Exhibit A).

7. Customer Proprietary Rights

7.1. Customer Content. As between Customer and Playlab, Customer owns all right, title, and interest in and to the Customer Content. Customer grants to Playlab a worldwide, non-exclusive, royalty-free limited license to access, use, copy, store, distribute, transmit, modify, perform, display, and create derivative works of Customer Content: (a) to provide, maintain, and update the Service; (b) to prevent or address service or technical problems; (c) as compelled by law; (d) as expressly permitted in writing signed by Customer; (e) to conduct impact research on the use of AI in educational settings for Playlab's internal business purposes only; (f) to create Performance Data and Aggregated and De-identified Data and to use such data during and after the Term, for any legal purpose, including to improve the Service and Playlab's offerings; and (g) to provide necessary access to third-party service providers acting on Playlab's behalf, such as providers of AI Features, *provided* that such Customer Content shall not be used by Playlab's providers as training data for AI models. With respect to any Community App, Customer grants to Playlab and other users a worldwide, non-exclusive, royalty-free, sublicensable, irrevocable, perpetual license to access, use, copy, store, distribute, transmit, modify, perform, display, and create derivative works of any Customer Content included in such Community App during and after the Term in order to make such Community App available on the Platform and to create Apps based on such Community App. Subject to the limited licenses granted herein, Playlab acquires no right, title or interest under this Agreement in or to any Customer Content.

8. Confidentiality

8.1. Definition. "***Confidential Information***" means all confidential information disclosed by a Party ("***Disclosing Party***") to the other Party ("***Receiving Party***"), whether orally or in writing, that is designated as confidential or that reasonably should be understood to be confidential given the nature of the information and the circumstances of disclosure, including all copies thereof. Confidential Information of Playlab includes the non-public aspects of the Service. Confidential Information will not include any information that: (a) is or becomes generally available to the public without breach of any obligation owed to the Disclosing Party; (b) was known to the Receiving Party prior to its disclosure by the Disclosing Party without breach of any obligation owed to the Disclosing Party; (c) is received from a third party without breach of any obligation owed to the Disclosing Party; (d) was independently developed by the Receiving Party without use of or reliance on the Confidential Information of the Disclosing Party; or (e) consists of Customer Content used in connection with, or used to develop, a Community App or an App that later becomes a Community App.

8.2. Customer Confidential Information: The Parties agree to abide by all applicable foreign and domestic laws, governmental regulations, ordinances, and judicial administrative orders in connection with the performance of its obligations hereunder, including, but not limited to, trademark and copyright laws, privacy laws, the United States Foreign Corrupt Practices Act, 15 U.S.C. § 78dd-1, et seq., and anti-bribery laws

(collectively "Applicable Laws"). Playlab affirms, acknowledges and understands that certain users of its Services will be the Customer's students who have not obtained the age of eighteen (18). Playlab agrees that it will abide by the Federal Education Rights and Privacy Act ("FERPA") and the Texas Education Code ("TEC") as it relates to all personally identifiable information or information that is linked to personally identifiable information, in any media or format, that is not publicly available concerning students, staff, administrators, vendors, and other third parties ("Covered Information") that is made available, intentionally or unintentionally, through the Customer's use of the Services. Playlab affirms and agrees that it has read, reviewed, and understands TEC § 32.001 *et seq*. concerning Operators, Covered Information, and limitations on the use of Covered Information by Operators. All Covered Information shall be considered Confidential Information. Playlab agrees that upon the Customer's request to delete a student or students' Covered Information or other information under the control of the school district and/or maintained by Playlab, Playlab shall delete the information subject to the Customer's request not later than the 10th Business Day after the date the request is received. Playlab covenants that it will not sell, transmit, or transfer any of the Covered Information or data it receives to any third party as part of this Agreement

8.3. Protection. The Receiving Party will: (a) use the same degree of care that it uses to protect the confidentiality of its own Confidential Information of like kind (but in no event less than reasonable care); (b) not use any Confidential Information of the Disclosing Party for any purpose outside the scope of this Agreement; and (c) except as otherwise authorized by the Disclosing Party in writing, limit access to Confidential Information of the Disclosing Party to those of the Receiving Party's employees, contractors, and agents who need such access for purposes consistent with this Agreement and who are subject to confidentiality obligations at least as restrictive as those herein. The Receiving Party will provide prompt written notice to the Disclosing Party of any unauthorized use or disclosure of the Disclosing Party's Confidential Information. Upon request of the Disclosing Party during the Term, the Receiving Party will promptly return, or at the Disclosing Party's option destroy, any or all Confidential Information of the Disclosing Party in the Receiving Party's possession or under its control. This paragraph does not abrogate or amend any of the provisions in the above paragraphs but should be interpreted as additional remedies in case Confidential Information is inadvertently transmitted between the Parties.

8.4. Compelled Disclosure. The Receiving Party may access or disclose Confidential Information of the Disclosing Party if it is compelled by law to do so, *provided* the Receiving Party gives the Disclosing Party prior notice of such compelled access or disclosure (to the extent legally permitted) and reasonable assistance, at the Disclosing Party's expense, if the Disclosing Party wishes to contest the access or disclosure.

8.5. Privacy and Security. The Parties agree that they each will comply with their respective obligations as required under the Data Protection Addendum ("DPA"), attached as Exhibit A, which is incorporated into and forms part of this Agreement. To the extent the DPA conflicts with the provisions of this Agreement, the Agreement will prevail.

9. **DMCA Policy.** It is Playlab's policy to terminate access privileges of any user of the Service who repeatedly infringes copyright upon prompt notification to Playlab by the copyright owner or the copyright owner's legal agent. Without limiting the foregoing, if Customer and/or any Authorized User believes that its work has been copied and posted on the Service in a way that constitutes copyright infringement, please provide Playlab's Copyright Agent with the following information:

9.1. an electronic or physical signature of the person authorized to act on behalf of the owner of the copyright interest;

9.2. a description of the copyrighted work that user claims has been infringed;

9.3. a description of the location on the Service of the material that user claims is infringing;

9.4. user's address, telephone number and e-mail address;

9.5. a written statement by user that such user has a good faith belief that the disputed use is not authorized by the copyright owner, its agent or the law; and

9.6. a statement by user, made under penalty of perjury, that the above information in user's notice is accurate and that user is the copyright owner or authorized to act on the copyright owner's behalf.

Contact information for Playlab's Copyright Agent for notice of claims of copyright infringement is as follows: Playlab Education Inc., c/o Copyright Agent, Denise Sulit with email copy to denise@playlab.ai. This paragraph shall not serve to limit the Customer's right to seek injunctive or other relief through legal means, including filing a lawsuit for copyright infringement.

10. Representations, Warranties, and Disclaimers

10.1. Mutual Representations. Each Party represents that: (a) it is duly organized, validly existing, and in good standing under its jurisdiction of organization and has the right to enter into this Agreement; and (b) the execution, delivery, and performance of this Agreement are within the corporate powers of such Party and have been duly authorized by all necessary corporate action on the part of such Party, and constitute a valid and binding agreement of such Party.

10.2. Customer Warranty. Customer warrants that (a) it has obtained and will maintain all rights, consents, and permissions necessary for Customer to make available the Customer Content to Playlab for its use as contemplated herein; (b) the Customer Content does not include any of the following: (i) export controlled materials; or (ii) sensitive information such as data regulated by the Health Insurance Portability and Accountability Act, the Gramm Leach Bliley Act, or the EU General Data Protection Regulation or any successor laws; and (c) that no Customer Content will violate or infringe any third-party intellectual property, publicity, privacy or other rights, or any applicable laws.

10.3. Disclaimer. THE SERVICE AND ALL RELATED COMPONENTS AND MATERIALS ARE PROVIDED ON AN "AS IS" BASIS WITHOUT ANY WARRANTIES OF ANY KIND, AND PLAYLAB EXPRESSLY DISCLAIMS ANY AND ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, TITLE, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. PLAYLAB DOES NOT WARRANT THAT THE SERVICE WILL BE UNINTERRUPTED OR ERROR-FREE OR WILL MEET CUSTOMER'S OR ANY AUTHORIZED USERS' REQUIREMENTS.

THE SERVICE IS INTENDED AS AN OUTPUT GENERATION TOOL ONLY AND DOES NOT CONSTITUTE THE ADVICE OF A CERTIFIED OR QUALIFIED EDUCATIONAL PROFESSIONAL. PLAYLAB MAKES NO WARRANTY OR GUARANTY THAT THE OUTPUT OR APPS WILL PROVIDE ACCURATE, TAILORED, OR INFORMATIVE RESULTS. PLAYLAB DOES NOT REPRESENT OR WARRANT THAT THE OUTPUT OR APPS DO NOT INCORPORATE, INFRINGE OR MISAPPROPRIATE THE INTELLECTUAL PROPERTY OR PROPRIETARY RIGHTS OF ANY THIRD PARTY. CUSTOMER ACKNOWLEDGES AND AGREES THAT (A) THE AI FEATURES LEVERAGE THIRD-PARTY SERVICES AND THAT PLAYLAB IS NOT LIABLE, AND CUSTOMER WILL NOT SEEK TO HOLD PLAYLAB LIABLE, FOR THIRD-PARTY CONTENT AND SERVICES; AND
(B) THAT THE RISK OF INJURY FROM SUCH THIRD-PARTY CONTENT AND SERVICES RESTS ENTIRELY WITH CUSTOMER. CUSTOMER SHALL BE SOLELY RESPONSIBLE FOR CUSTOMER'S USE OF THE SERVICE, APPS, AND ANY OUTPUT RESULTING THEREFROM. CUSTOMER SHOULD EVALUATE THE FITNESS OF ANY OUTPUT OR APP AS APPROPRIATE FOR CUSTOMER'S SPECIFIC USE CASE.

11. Indemnification

11.1. Customer Indemnification. Customer will, to the extent permitted by applicable law, defend Playlab from and against any lawsuit or proceeding brought by a third party to the extent alleging (a) Customer's breach of Section 3.3 or 10.2, (b) that any Customer Content infringes, misappropriates, or otherwise violates the rights, including privacy and publicity rights, of any other party, or (c) Customer's or any Authorized User's use of the Service violates any applicable laws or government regulations. Customer agrees to indemnify Playlab for any damages and any reasonable attorneys' fees finally awarded against it arising from such lawsuit or proceeding; *provided*, *however*, that Customer will have no liability under this Section to the extent any such lawsuit or proceeding, or any part thereof, arises from Playlab's own acts or omissions, negligence, misconduct, or material breach of this Agreement.

11.2. Procedures. The indemnified Party will provide the indemnifying Party with: (a) prompt written notice of any matter that is subject to indemnification hereunder; (b) the right to assume the exclusive defense and control of any such matter (*provided* that the indemnified Party may participate in the defense at its own expense); and (c) cooperation with any reasonable requests assisting the indemnifying Party's defense of such matter. The indemnifying Party may not settle any such lawsuit or proceeding without the indemnified Party's prior written consent.

11.3. Exclusive Remedy. This Section 11 states the indemnifying Party's sole liability, and the indemnifying Party's exclusive remedy, for any type of claim described in this Section 11.

12. Limitation of Liability

12.1. Exclusion of Certain Damages. SUBJECT TO SECTION 12.3, IN NO EVENT WILL PLAYLAB HAVE ANY LIABILITY TO CUSTOMER OR TO ANY OTHER PARTY FOR ANY LOST PROFITS OR REVENUES OR FOR ANY INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, COVER, OR PUNITIVE DAMAGES, WHETHER OR NOT PLAYLAB HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE FOREGOING DISCLAIMER WILL NOT APPLY TO THE EXTENT PROHIBITED BY APPLICABLE LAW.

12.2. Liability Cap. SUBJECT TO SECTION 12.3, IN NO EVENT WILL PLAYLAB'S AGGREGATE LIABILITY RELATING TO THIS AGREEMENT EXCEED THE AMOUNTS PAID IN THE TWELVE (12) MONTHS PRECEDING THE FIRST INCIDENT OUT OF WHICH THE LIABILITY AROSE.

12.3. Exclusions. THE LIMITATIONS OF LIABILITY IN SECTION 12.1 AND THE CAP ON LIABILITY IN SECTION 12.2 DO NOT APPLY TO (A) DAMAGES ARISING FROM A BREACH BY A PARTY OF SECTION 3.3, 3.5, 8, OR 10.2; (B) A PARTY'S INDEMNIFICATION OBLIGATIONS UNDER SECTION 11; AND (C) EITHER PARTY'S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT,

12.4. Scope. For the avoidance of doubt, the exclusions and limitations set forth in this Section 12 will apply with respect to all legal theories of liability, whether in contract, tort, or otherwise. The Parties agree that the exclusions and limitations set forth in this Section 12 allocate the risks between the Parties under this Agreement, and that they have relied on these exclusions and limitations in determining whether to enter into this Agreement.

13. Term, Termination, and Suspension

13.1. Term of the Agreement. The term of this Agreement commences on the Effective Date and, unless earlier terminated in accordance with the terms of this Agreement, will continue for a one (1) year (the "***Initial Term***"). Thereafter, this Agreement (including the Statement of Work) will automatically renew for successive additional periods of one (1) year each (each, a "***Renewal Term***") unless either Party provides the other with written notice of non-renewal at least thirty (30) days prior to the expiration of the Initial Term or the then-current Renewal Term. Customer agrees that Playlab may implement or modify the Fees for each Renewal Term by providing Customer with written notice of such modification at least thirty (30) days prior to the expiration of the Initial Term or the then-current Renewal Term, as applicable. The Initial Term and each Renewal Term, if any, are collectively referred to herein as the "***Term***." The automatic renewals referenced in this paragraph may not occur more than three (3) times without the Parties entering into another written agreement. If no Agreement is timely signed, then the Agreement terminates.

13.2. Suspension. Playlab may suspend Customer's or any or all Authorized Users' access to the Service, in whole in part, if: (a) Customer or any Authorized User is using the Service in violation of this Agreement or any applicable law; (b) Customer's or any Authorized Users' systems or accounts have been compromised or unlawfully accessed; (c) suspension of the Service is necessary, in Playlab's reasonable discretion, to protect the security of the Service or Playlab's infrastructure; (d) suspension is required by applicable law; or (e) if applicable, any Fees owed by Customer (excluding amounts disputed in reasonable and good faith) are thirty
(30) days or more overdue.

13.3. Termination for Cause. Either Party may terminate this Agreement effective after thirty (30) days' written notice if the other Party materially breaches this Agreement and such breach is not cured within such thirty (30)-day period. Upon any termination for cause by Customer, Playlab will promptly refund Customer any prepaid Fees covering the period remaining in the Term after the effective date of such termination. Upon any termination for cause by Playlab, Customer will promptly pay Playlab any unpaid Fees covering the period remaining in the Term after the effective date of such termination.

13.4. Effects of Termination. In no event will any termination of this Agreement relieve Customer of its obligation (if applicable) to pay any Fees payable to Playlab for the period of time prior to the effective date of such termination. Upon any termination of this Agreement, Customer's and all Authorized Users' access and use of the Service may be downgraded to the access permissions of a free account or be otherwise limited by Playlab in its sole discretion. Playlab may remove any Apps embedded on a Customer Website via the Embedding Feature in its sole discretion. For a period of thirty (30) days following any termination of this Agreement, Playlab will, upon Customer's request, provide Customer with an export of all current Customer Content in the format agreed by the Parties. After such thirty (30)-day period, Playlab will have no obligation to maintain or provide any Customer Content and Playlab may, unless prohibited by applicable law, delete all Customer Content in its systems or otherwise in its possession or under its control in accordance with Playlab's then-current data retention and deletion policies. Subject to this Section, upon any termination of this Agreement and the Disclosing Party's request, the Receiving Party will promptly return, or at the Disclosing Party's option destroy, any or all Confidential Information of the Disclosing Party in the Receiving Party's possession or under its control.

13.5. Survival. The following sections will survive any termination or expiration of this Agreement: 1, 3.5, 3.6, 5, 6, 7.1 (with respect to the last sentence), 8, 10, 11, 12, 13.4, 14, and 15.

14. **Dispute Resolution & Governing Law.** This Agreement and any dispute arising from or relating to this Agreement are governed by the laws of the State of Texas, United States, without regard to its conflict of law principles. To the extent the Parties are permitted under this Agreement to initiate litigation in court, the Parties' consent to exclusive personal jurisdiction and venue in the courts located in Ector County, Texas. The Parties agree that this Agreement was drafted and is performable in Ector County, Texas. Any breach of this Agreement shall occur in Ector County, Texas.

15. General Provisions

15.1. Force Majeure. Neither Party will be liable hereunder by reason of any failure or delay in the performance of its obligations due to events beyond the reasonable control of such Party, which may include natural disasters, fires, epidemics, pandemics, riots, war, terrorism, denial of service attacks, internet outages, labor shortages, and judicial or government action.

15.2. Assignment. Neither Party may assign any of its rights or obligations hereunder, whether by operation of law or otherwise, without the prior written consent of the other Party. Notwithstanding the foregoing, either Party may assign or transfer this Agreement in its entirety, without the consent of the other Party, in connection with a merger or sale of all or substantially all of its assets. Any purported assignment in violation of this Section will be null and void. This Agreement will bind and inure to the benefit of the Parties, their respective successors, and permitted assigns.

15.3. Export Control. In its use of the Services, Customer agrees to comply with all export and import laws and regulations of the United States and other applicable jurisdictions. Without limiting the foregoing, (a) Customer represents and warrants that it is not listed on any U.S. government list of prohibited or restricted parties or located in (or a national of) a country that is subject to a U.S. government embargo or that has been designated by the U.S. government as a "terrorist supporting" country, (b) Customer will not (and will not permit any of its users to) access or use the Services in violation of any U.S. export embargo, prohibition or restriction, and (c) Customer will not submit to the Services any information that is controlled under the U.S. International Traffic in Arms Regulations.

15.4. Notices. All notices under this Agreement will be in writing and (a) if to Customer, addressed to Customer at the addresses set forth on the Statement of work and (b) if to Playlab, at 33170 Alvarado

Niles Rd #3048 Union City, CA 94587, and will be deemed to have been duly given: (i) upon receipt if personally delivered or sent by certified or registered mail with return receipt requested; or (ii) the first business day after sending by email or by next day delivery by a recognized overnight delivery service.

15.5. Relationship of the Parties; Third-Party Beneficiaries. The Parties are independent contractors, and this Agreement does not create a partnership, franchise, joint venture, agency, fiduciary, or employment relationship between the Parties. There are no third-party beneficiaries to this Agreement.

15.6. Waiver. No failure or delay by either Party in exercising any right under this Agreement will constitute a waiver of that right.

15.7. Severability. If any provision of this Agreement is held by a court of competent jurisdiction to be invalid or unenforceable, such provision will be modified by the court and interpreted so as best to accomplish the objectives of the original provision to the fullest extent permitted by law, and the remaining provisions of this Agreement will remain in full force and effect.

15.8. Subcontractors. Playlab may use one or more third parties to fulfill any of its obligations hereunder, *provided* that with respect to any such obligations that are subcontracted to or provided by any third party, Playlab expressly assumes all liability and responsibility for such third party's compliance with, including, without limitation, any breach of, the terms of this Agreement.

15.9. Entire Agreement. This Services Agreement, including any Exhibits hereto and all Statement of works, constitute the entire agreement between the Parties and supersede all prior and contemporaneous agreements, proposals, or representations, written or oral, concerning the subject matter hereof. No modification, amendment, or waiver of any provision of an Statement of work will be effective unless in writing and signed by each of the Parties. Playlab may modify this Services Agreement on a going-forward basis from time to time by posting the modified Services Agreement to https://www.playlab.ai/policies/ and any such modifications will take effect upon renewal of the then-current Term so long as Playlab has provided the Customer with written notice of the changes. To the extent of any conflict or inconsistency between the Services Agreement or any Statement of work, the terms set forth in the Services

Agreement will control unless the conflicting term in the other document specifically references the inconsistent term of the Services Agreement, in which case the conflicting term will control only for the limited purposes set forth in the document containing such term. Notwithstanding any language to the contrary therein, no terms or conditions stated in any Customer purchase order or other Customer order documentation (excluding Statement of works) will be incorporated into or form any part of this Agreement, and all such terms or conditions will be null and void. As used herein, the words "include" and "including" shall be deemed to be followed by the words "without limitation." Titles and headings of sections are for convenience only and shall not affect the construction of any provision of this Agreement.

SIGNATURE PAGE

PLAYLAB EDUCATION INC.

By: 

Name: Denise Sulit

Title: Operations Manager

Date: 04 / 21 / 2026

ECTOR COUNTY INDEPENDENT SCHOOL DISTRICT

By: _____

Name: _____

Title: _____

Date: _____

EXHIBIT A: DPA

TX-NDPA-V1

STANDARD STUDENT DATA PRIVACY AGREEMENT

TX-NDPA v1r6

School District or LEA

Ector County Independent School District

and

Provider

Playlab Education, Inc.

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:

[Ector County Independent School District], located at [802 N. Sam Houston, Odessa, TX 79761] (the "**Local Education Agency**" or "**LEA**") and

[Playlab Education, Inc.], located at [33170 Alvarado Niles Rd #3048 Union City, CA] (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, LEA and Provider agree to the additional terms or modifications set forth in **Exhibit "H". (Optional)**
   - ☐ 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 (3) years. **Exhibit "E"** will expire three (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:_____ Title: _____

Address: _____

Phone:_____ Email: _____

The designated representative for the Provider for this DPA is:

Name: Denise Sulit Title: Operations Manager

Address: 33170 Alvarado Niles Rd #3048 Union City, CA 94587

Phone: 7325891380 Email: denise@playlab.ai

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

LEA:

By:_____ Date: _____

Printed Name:_____ Title/Position: _____

Provider:

By:  Date: 3/30/2026

Printed Name: Denise Sulit Title/Position: Operations Manager

STANDARD CLAUSES

Version 1.0

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 the 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 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

Playlab is an educational platform that empowers educators and impact organizations to build their own tools powered by Artificial Intelligence (AI). The platform is specifically designed for educational use cases and adheres to applicable privacy laws including FERPA and COPPA.

Key services include:

Creation of custom AI-powered educational tools
Individual and organizational accounts for educational purposes
Support for a wide range of learning use cases, both in and outside of school contexts
Features that allow educators to work with students, provide education-related services, and evaluate educational achievement
Tools that help educators develop AI applications without requiring technical expertise
Playlab is committed to educational purposes only and prohibits use of their services for non-educational purposes, commercial exploitation, or any activities that violate their Usage Policy.

EXHIBIT "B"

SCHEDULE OF DATA

Category of Data	Elements	Check if Used by Your System
Application Technology Meta Data	IP Addresses of users, Use of cookies, etc.	☑
	Other application technology meta data-Please specify: time zone, country, access times	☑
Application Use Statistics	Meta data on user interaction with application	☑
Assessment	Standardized test scores	☐
	Observation data	☑
	Other assessment data-Please specify: school-related performance data	☑
Attendance	Student school (daily) attendance data	☐
	Student class attendance data	☐
Communications	Online communications captured (emails, blog entries)	☑
Conduct	Conduct or behavioral data	☐
Demographics	Date of Birth	☐
	Place of Birth	☐
	Gender	☐
	Ethnicity or race	☐
	Language information (native, or primary language spoken by student)	☑

Category of Data	Elements	Check if Used by Your System
	Other demographic information-Please specify:	☐
Enrollment	Student school enrollment	☐
	Student grade level	☑
	Homeroom	☐
	Guidance counselor	☐
	Specific curriculum programs	☐
	Year of graduation	☐
	Other enrollment information-Please specify:	☐
Parent/Guardian Contact Information	Address	☐
	Email	☐
	Phone	☐
Parent/Guardian ID	Parent ID number (created to link parents to students)	☐
Parent/Guardian Name	First and/or Last	☐
Schedule	Student scheduled courses	☐
	Teacher names	☐
Special Indicator	English language learner information	☐
	Low income status	☐
	Medical alerts/ health data	☐

Category of Data	Elements	Check if Used by Your System
	Student disability information	☐
	Specialized education services (IEP or 504)	☐
	Living situations (homeless/foster care)	☐
	Other indicator information-Please specify:	☐
Student Contact Information	Address	☐
	Email	☑
	Phone	☐
Student Identifiers	Local (School district) ID number	☐
	State ID number	☐
	Provider/App assigned student ID number	☐
	Student app username	☑
	Student app passwords	☑
Student Name	First and/or Last	☑
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	☑
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	☐
Student Survey Responses	Student responses to surveys or questionnaires	☑
Student work	Student generated content; writing, pictures, etc.	☑

Category of Data	Elements	Check if Used by Your System
	Other student work data -Please specify:	☐
Transcript	Student course grades	☐
	Student course data	☐
	Student course grades/ performance scores	☐
	Other transcript data - Please specify:	☐
Transportation	Student bus assignment	☐
	Student pick up and/or drop off location	☐
	Student bus card ID number	☐
	Other transportation data – Please specify:	☐
Other	Please list each additional data element used, stored, or collected by your application: Usage data including features used, time spent on platform, device information	☑
None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	☐

EXHIBIT "C"

DEFINITIONS

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

Educational Records: Educational Records are records, files, documents, and other materials directly related to a student and maintained by the school or local education agency, or by a person acting for such school or local education agency, including but not limited to, records encompassing all the material kept in the student's cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs.

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

Operator: means the operator of an internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used for K–12 school purposes. Any entity that operates an internet website, online service, online application, or mobile application that has entered into a signed, written agreement with an LEA to provide a service to that LEA shall be considered an "operator" for the purposes of this section.

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

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

Student Generated Content: The term "Student-Generated Content" means materials or content created by a student in the services including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of student content.

School Official: For the purposes of this DPA and pursuant to 34 CFR § 99.31(b), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of Student Data including Education Records; and (3) Is subject to 34 CFR § 99.33(a) governing the use and re-disclosure of Personally Identifiable Information from Education Records.

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

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data includes Meta Data. Student Data further includes "Personally Identifiable Information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local laws and regulations. Student Data as specified in **Exhibit "B"** is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or De-Identified, or anonymous usage data regarding a student's use of Provider's services.

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

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

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

Third Party: The term "Third Party" means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Education Records and/or Student Data, as that term is used in some state statutes. However, for the purpose of this DPA, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF DATA

Provider to dispose of data obtained by Provider pursuant to the termsof 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 Provider Date

EXHIBIT "E"

GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and [Ector County Independent School District] ("Originating LEA") which is dated [3/30/2026], 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 statues; (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: denise@playlab.ai

[NAME OF PROVIDER]

BY: Playlab Education, Inc. Date: 3/30/2026

Printed Name: Denise Sulit Title/Position: Operations Manager

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 [Ector County Independent School District] and the Provider. **PRIOR TO ITS EFFECTIVENESS, SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER PURSUANT TO ARTICLE VII, SECTION 5. **

Subscribing 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

The Education Security and Privacy Exchange ("Edspex") works in partnership with the Student Data Privacy Consortium and industry leaders to maintain a list of known and credible cybersecurity frameworks which can protect digital learning ecosystems chosen based on a set of guiding cybersecurity principles* ("Cybersecurity Frameworks") that may be utilized by Provider .

Cybersecurity Frameworks

	MAINTAINING ORGANIZATION/GROUP	FRAMEWORK(S)
☑	National Institute of Standards and Technology (NIST)	NIST Cybersecurity Framework Version 1.1
☑	National Institute of Standards and Technology (NIST)	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
☑	International Standards Organization (ISO)	Information technology — Security techniques — Information security management systems (ISO 27000 series)
☐	Secure Controls Framework Council, LLC	Security Controls Framework (SCF)
☐	Center for Internet Security (CIS)	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)

Please visit http://www.edspex.org for further details about the noted frameworks.

*Cybersecurity Principles used to choose the Cybersecurity Frameworks are located here

EXHIBIT "G"

Supplemental SDPC State Terms for Texas

Version 1.0

This **Exhibit "G"**, Supplemental SDPC State Terms for Texas ("Supplemental State Terms"), effective simultaneously with the attached Student Data Privacy Agreement ("DPA") by and between [Ector County Independent School District] (the "Local Education Agency" or "LEA") and [Playlab Education, Inc.] (the "Provider"), is incorporated in the attached DPA and amends the DPA (and all supplemental terms and conditions and policies applicable to the DPA) as follows:

1. **Covered Data.** All instances of "Student Data" should be replaced with "LEA Data". The protections provided within this DPA extend to all data provided to or collected by the Provider.

2. **Compliance with Texas Privacy Laws and Regulations.** In performing their respective obligations under the Agreement, the LEA and the Provider shall comply with all Texas laws and regulations pertaining to LEA data privacy and confidentiality, including but not limited to the Texas Education Code Chapter 32, and Texas Government Code Chapter 560.

3. **Modification to Article III, Section 2 of the DPA.** Article III, Section 2 of the DPA (Annual Notification of Rights.) is amended as follows:

   ~~**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.~~
   Consider Provider as School Official. The Parties agree that Provider is a "school official" under FERPA and has a legitimate educational interest in personally identifiable information from education records received from the LEA pursuant to the DPA. For purposes of the Service Agreement and this DPA, Provider: (1) provides a service or function for which the LEA would otherwise use employees; (2) is under the direct control of the LEA with respect to the use and maintenance of education records; and (3) is subject to the requirements of FERPA governing the use and redisclosure of personally identifiable information from the education records received from the LEA.

4. **Modification to Article V, Section 4 of the DPA.** Article V, Section 4 of the DPA (Data Breach.) is amended with the following additions: (6) For purposes of defining an unauthorized disclosure or security breach, this definition specifically includes meanings assigned by Texas law, including applicable provisions in the Texas Education Code and Texas Business and Commerce Code. (7) The LEA may immediately terminate the Service Agreement if the LEA determines the Provider has breached a material term of this DPA. (8) The Provider's obligations shall survive termination of this DPA and Service Agreement until all Data has been returned and/or Securely Destroyed.

5. **Modification to Article VII, Section 4 of the DPA.** Article VI, Section 4 of the DPA (Annual Notification of Rights.) is amended as follows:

   Entire Agreement. This DPA ~~and the Service Agreement~~ constitutes the entire agreement of the Parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the Parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both Parties. Neither failure nor delay on the part of any Party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.

6. **Reimbursement of Expenses Associated with Security Breach.** In the event of a Security Breach that is attributable to the Provider, the Provider shall reimburse and indemnify the LEA for any and all costs and expenses that the LEA incurs in investigating and remediating the Security Breach, including but not limited to costs and expenses associated with:

   a. Providing notification to the employees or parents of those students whose LEA Data was compromised and regulatory agencies or other entities as required by law or contract;

   b. Providing credit monitoring to those employees or students whose LEA Data was exposed in a manner during the Security Breach that a reasonable person would believe may impact the employee's or student's credit or financial security;

   c. Legal fees, audit costs, fines, and any other fees or damages imposed against the LEA as a result of the security breach; and

   d. Providing any other notifications or fulfilling any other requirements adopted by the Texas State Board of Education, Texas Education Agency, or under other State or federal laws.

7. **No Exhibit E without unaltered DPA including Texas Addendum.** Any alterations are only allowed in **Exhibit "H"**. Any terms under **Exhibit "H"** do not apply to **Exhibit "E"** and render **Exhibit "E"** null and void.

EXHIBIT "H"

Additional Terms or Modifications

Version

LEA and Provider agree to the following additional terms and modifications:

None

Annex 1 Security

Measures

As from the Effective Date, Playlab will implement and maintain the Security Measures as set out in this Annex. Playlab's failure to implement and maintain the Security Measures shall be considered a material breach of this Agreement.

1. Organizational management and dedicated staff responsible for the development, implementation and maintenance of Playlab's information security program.

2. Audit and risk assessment procedures for the purposes of periodic review and assessment of risks to Playlab's organization, monitoring and maintaining compliance with Playlab's policies and procedures, and reporting the condition of its information security and compliance to internal senior management.

3. Data security controls which include at a minimum: logical segregation of data, restricted (e.g., role-based) access and monitoring, and utilization of commercially reasonable encryption technologies for Personal Data.

4. Logical access controls designed to manage electronic access to data and system functionality, based on authority levels and job functions.

5. Password controls designed to manage and control password strength, expiration and usage.

6. System audit or event logging and related monitoring procedures to proactively record Authorized User access and system activity.

7. Physical and environmental security of data centers, server room facilities and other areas containing Personal Data designed to protect information assets from unauthorized physical access or damage.

8. Operational procedures and controls to provide for configuration, monitoring and maintenance of technology and information systems, including secure disposal of systems and media to render all information or data contained therein as undecipherable or unrecoverable prior to final disposal or release from Playlab's possession.

9. Change management procedures and tracking mechanisms designed to test, approve and monitor all material changes to Playlab's technology and information assets.

10. Incident management procedures designed to allow Playlab to investigate, respond to, mitigate and notify of events related to Playlab's technology and information assets.

11. Network security controls that provide for the use of enterprise firewalls and intrusion detection systems designed to protect systems from intrusion and limit the scope of any successful attack.

12. Vulnerability assessment and threat protection technologies and scheduled monitoring procedures designed to identify, assess, mitigate and protect against identified security threats, viruses and other malicious code.

13. Business resiliency/continuity and disaster recovery procedures designed to maintain service and/or recovery from foreseeable emergency situations or disasters.

EXHIBIT B: STATEMENT OF WORK

PSP + ECISD + Playlab Partnership Proposal

(ECISD Shared Learning Series + Regional Capacity Building)

Overview

PSP and Playlab propose a focused partnership with ECISD to build practical AI capacity through a **Shared Learning Series** that includes up to 40 ECISD participants, as well as representatives from ESCs and Teacher Prep Programs. This initiative also includes licenses for builder accounts, Clever integration for unlimited students, and targeted supports such as site visits and light custom app creation.

The goal is to empower educators, leaders, and regional partners to move from AI exploration to meaningful implementation by aligning AI use with district priorities, High-Quality Instructional Materials (HQIM), and measurable outcomes. This program represents a regional investment in capacity-building and innovation to ensure sustainable AI adoption across ECISD and beyond.

Goals & Outcomes

Goal 1: Strengthen Educator AI Literacy Through Hands-On Learning

- Increased confidence among educators, leaders, and regional partners in using AI for planning, instruction, operations, and coaching.
- Priority use cases identified and scoped for ECISD and regional contexts.
- Starter tools/apps co-developed and piloted in live settings.

Goal 2: Drive Strategic, Measurable AI Adoption

- Development of **3–5 shared high-quality apps** addressing ECISD and regional priorities.
- Each participant will create their own app aligned to their specific needs or use cases.
- Clear entry points and guardrails for sustainable AI implementation.
- Early evidence of time-saved, quality gains, or learning impacts in targeted areas.

Goal 3: Build a Regional Network for Sustainable AI Adoption

- Inclusion opportunities for ESC representatives and Teacher Prep Programs to extend learning and capacity across the region.
- Shared artifacts and training materials to support regional scaling.
- Strengthened collaboration among ECISD, ESCs, and Teacher Prep Programs to align AI use with educational goals in West Texas.

Program Structure (What's Included)

A. Shared Learning Series (4–6 Sessions, Free for All Participants)

- **Audience**: ECISD leaders, coaches, teacher-leaders, central office staff, ESC representatives, and Teacher Prep Program participants.
- **Format**: Action-oriented workshops (virtual/in-person mix) combining AI literacy, tool demonstrations, and build time.
- **Focus Areas** (co-selected with ECISD):
  - HQIM-aligned planning supports and teacher-facing tools.
  - Instructional coaching and observation supports.
  - Student-facing feedback and practice tools.
  - Operational workflows (e.g., registrar processes, family communications, translations).
- **Outputs**:
  - Use-case briefs.
  - **3–5 shared high-quality apps** developed and tested in regional settings.
  - Each participant will create and test their own app.

B. Site Visits & Walkthroughs

- **1–2 site visits** to observe classrooms/systems, gather user stories, and model AI use in real settings.
- Optional cross-campus or cross-role shadowing for leaders/coaches.
- To the extent Playlab's agents or representatives are required to interact, directly or indirectly, with ECISD students or other students, Playlab shall abide by all applicable laws concerning criminal background checks, criminal disclosures, and information provision prior to such interaction. This section applies to the Agreement and each subsection of the SOW.

C. Custom App Creation (Light Build)

- **1–3 priority tools/apps** scoped with ECISD and built or adapted on Playlab's platform.
- Includes user testing and rapid iteration.

D. Regional Participation

- Reserved seats for ESC representatives and Teacher Prep Programs to join the Shared Learning Series and community of practice.
- This ensures alignment and sustainability across regional educational systems.

Progress

E. Enterprise Software License (Included)

- Full access to Playlab's AI platform for all participants (builder accounts for educator/leader use).
- Unlimited Clever integration for ECISD students.
- Access to curriculum-aligned and custom knowledge libraries.

- Multi-model support (e.g., ChatGPT, Claude, Gemini) with built-in safeguards.
- Advanced sharing options, permissions management, analytics dashboard, and admin support.

Roles & Responsibilities

ECISD:

- Identify participants (up to 40 for ECISD) and coordinate with ESCs and Teacher Prep Programs.
- Set goals and provide access to relevant HQIM/resources.
- Coordinate schedules and site access.

Playlab:

- Design and facilitate the Shared Learning Series.
- Provide platform access, documentation, and office hours.
- Lead app scoping/builds and support implementation.

Permian Strategic Partnership

- Convene/support partners, including ESCs and Teacher Prep Programs.
- Facilitate cross-institution collaboration and regional learning capture.
- Secure funding to ensure program sustainability and support.
- To the extent the PSP's agents or representatives are required to interact, directly or indirectly, with ECISD students or other students, the PSP shall abide by all applicable laws concerning criminal background checks, criminal disclosures, and information provision prior to such interaction. This section applies to the Agreement and each subsection of the SOW.
-

Success Measures

- **Participation:** ≥80% attendance across sessions, including ESC and Teacher Prep Program representatives.
- **Implementation:** Development of **3–5 shared high-quality apps** addressing ECISD and regional priorities. Each participant will design and test their own app.
- **Efficiency/Quality: Documented** evidence of time savings (e.g., planning/coaching) or quality gains (e.g., clearer feedback, stronger lesson internalization).
- **Sustainability:** Regional plan for capacity-building and AI scaling, including ESC and Teacher Prep Program participation.

Logistics

To be finalized in a **60-minute planning call**, covering:

- Final goals and success criteria.
- Participant list and roles (leaders, ESC representatives, Teacher Prep Programs).

- Session cadence (4–6 total), modality (virtual/in-person), and dates.
- Priority app shortlist and site visit windows.

Total Investment

Service	Description	Cost
Shared Learning Series	Action-oriented PD series (4–6 sessions) for ECISD, ESC, and Teacher Prep participants, including all builder licenses and materials.	**Included**
Enterprise Software License	Platform access for all participants, Clever integration for students, and access to libraries, dashboards, and admin support.	**Included**
Coaching, Site Visits & Custom Builds	Bi-weekly check-ins, monthly office hours, 1–2 site visits, ~20 hours of app development, and documentation.	**Included**

Total Cost of Program: $250,000

(Covers all services, licenses, and supports for ECISD, ESC, and Teacher Prep Program participants.)

Let's Build Together

This partnership represents a regional investment in education innovation, empowering ECISD, ESCs, and Teacher Prep Programs to lead the way in responsible AI adoption. By collaborating across institutions and sharing resources, we will create practical tools, sustainable systems, and measurable outcomes that benefit students, educators, and communities in West Texas.