

Standard Student Data Privacy Agreement

Special Instructions for Form Completion

Enclosed within this communication, you will find a template for the Data Privacy Agreement (DPA). Note that all references to page numbers below pertain to the pages in the attached fillable PDF document.

Please be advised that the individual signing the DPA must possess the requisite authority to bind your organization to the terms and conditions outlined within the Data Privacy Agreement. Additionally, any alterations to the document's content outside of the designated fillable text fields—commonly referred to as "redlining"—will necessitate a comprehensive legal review. Such actions are likely to introduce further delays in the finalization process.

Page number	Section/Reference	Guidance
1	(Blank field)	Legal name of the organization, plus any DBA
2	a. (1 st Blank field) b. (2 nd Blank field) c. (Section 2 – Special provisions. 1st checkbox)	a. Legal name of entity, plus any DBA. b. Official address. c. Determine whether the organization wants to use Exhibit E to offer this SDPA to other districts within Texas. - If YES, then check the box under “Special Provisions.”
3	Provider designee name and contact information	“The designated representative for the Provider for this DPA is”: this may be the organization’s authorized signatory, but it could be the project manager or for this relationship. Point of Contact name and title.
10	Signature page	Provider signature, please fill in and sign.
11	Exhibit A Description of Services	A1 and A2 description of services and scope of work
12-15	Exhibit B Proposed Schedule of Data	Proposed list of standard data elements needed and collected, check all that apply.
19	Exhibit D Disposition of Data	Complete items 1, 2, and 3 now based on the terms identified by the vendor. HISD will sign item 4 on Exhibit D when we execute it. Vendor will receive the signed copy as part of the fully executed agreement. At the end of contract or relationship period the vendor will provide a copy of Exhibit D with vendor signatures once the vendor destroys the data.
21	Exhibit F Data Security Requirements	Check all that apply, must check at least one
22	Exhibit G Supplemental SDPC State Terms for Texas	Legal name of the organization, plus any DBA
24	Exhibit H Additional Terms or Modifications	2A Ethics and Compliance Checkboxes 2B Cybersecurity checkboxes
27	Contractor Criminal History Background Check Certification	The vendor is required to complete the background check form to attest if the vendor will have contact with students. If “NO” in section I, skip section II, complete and sign section III.



Texas Student Privacy Alliance

STANDARD STUDENT DATA PRIVACY AGREEMENT

SDPC TX-NDPA v1r6

HOUSTON INDEPENDENT SCHOOL DISTRICT

and

© Access 4 Learning (A4L) Community. All Rights Reserved.

This document may only be used by A4L Community members and may not be altered in any substantive manner.

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:

Houston Independent School District, located at 4400 West 18th St Houston Texas 77092 (the “**Local Education Agency**” or “**LEA**” or “**District**”) and

_____, located at *Address of Provider* (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 Provider has signed **Exhibit “E”** to the Standard Clauses, otherwise known as General Offer of Privacy Terms
 - ☒ 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”**.
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 or “Business Owner” for the LEA for this DPA is:

Name: _____ Title: _____

Address: _____

Phone: _____ Email: _____

The designated representative for the Provider for this DPA is:

Name: _____ Title: _____

Address: _____

Phone: _____ Email: _____

STANDARD CLAUSES

Texas-NDPA Version 1.0 Rev. 6

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 Article II section 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 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.

HOUSTON INDEPENDENT SCHOOL DISTRICT

REQUESTOR'S SIGNATURE:

By: **Tanya Pridgeon**

Date

*Executive Director IT Data Governance*By: **Matthew Sawyer**

Date

Deputy Chief of Data and Impact

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

By:

*Name - Authorized Representat

Date

*Title - Authorized Representativ

Taxpayer Identification Number

HOUSTON INDEPENDENT SCHOOL DISTRICT

By:

Heather Hughes
Controller

Date

APPROVED AS TO FORM:

Erica Graham
Deputy General Counsel

Date

<OR>

Miles J. LeBlanc
Assistant General Counsel

Date

<OR>

Fei Berkeley
Assistant General Counsel

Date

EXHIBITS

Texas-NDPA Version 1.0 Rev. 6

EXHIBIT “A” DESCRIPTION OF SERVICES

Required: Provider’s Services and Activities.

A1. Describe the Provider’s standard data sharing mechanism and protocols. 600-character limit.

A2. Summarize the Activities authorized by LEA in the documents attached. 1800-character limit.

Suggested Attachments to Exhibit A to document authorization of Provider’s Services may include:

- A PDF of the LEA board item(s) from the Agenda Packet when Services/Activities were approved, plus Published minutes showing the DATE and RESULT of the vote
- A PDF of previously executed contract(s)
- A PDF of Scope of Work approved by LEA “Business Owner” or LEA “Purchasing” for this specific Project

These attachments do not count against character limits.

EXHIBIT “B” PROPOSED SCHEDULE OF DATA

Data elements checked below are confirmed to be collected by or to be requested by the Provider pursuant to the Services described in **Exhibit A**.

Category of Data	Elements	Check if Collected by Your System	Check if Requesting from LEA
(01) Application Technology Meta Data	IP Addresses of users, Use of cookies, etc.	☐	☐
	Other application technology meta data — Please specify: 	☐	☐
(02) Application Use Statistics	Meta data on user interaction with application	☐	☐
(03) Assessment	Standardized test scores	☐	☐
	Observation data	☐	☐
	Other assessment data — Please specify:	☐	☐
(04) Attendance	Student school (daily) attendance data	☐	☐
	Student class attendance data	☐	☐
(05) Communications	Online communications captured (emails, blog entries)	☐	☐
(06) Conduct	Conduct or behavioral data	☐	☐
(07) 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 Collected by Your System	Check if Requesting from LEA
	Other demographic information — Please specify: 	☐	☐
(08) Enrollment	Student school enrollment	☐	☐
	Student grade level	☐	☐
	Homeroom	☐	☐
	Guidance counselor	☐	☐
	Specific curriculum programs	☐	☐
	Year of graduation	☐	☐
	Other enrollment information — Please specify: 	☐	☐
(09) Parent/Guardian Contact Information	Address	☐	☐
	Email	☐	☐
	Phone	☐	☐
(10) Parent/Guardian ID	Parent ID number (created to link parents to students)	☐	☐
(11) Parent/Guardian Name	First and/or Last	☐	☐
(12) Schedule	Student scheduled courses	☐	☐
	Teacher names	☐	☐
(13) Special Indicator	English Language Learner or Emergent Bilingual status	☐	☐
	Low-income status	☐	☐
	Medical alerts/ health data	☐	☐

Category of Data	Elements	Check if Collected by Your System	Check if Requesting from LEA
	Student disability information	☐	☐
	Specialized education services (IEP or 504)	☐	☐
	Living situations (homeless/foster care)	☐	☐
	Other information — Please specify: 	☐	☐
(14) Student Contact Information	Address	☐	☐
	Email	☐	☐
	Phone	☐	☐
(15) Student Identifiers	Local (School district) ID number	☐	☐
	State ID number	☐	☐
	Provider/App assigned student ID number	☐	☐
	Integration with Single Sign On (SSO)	☐	☐
	Student username unique to application	☐	☐
	Student password unique to application	☐	☐
(16) Student Work in App	Program/application performance (typing program- student types 60 wpm, reading program-student reads below grade level)	☐	☐
(17) Student Name	First, Middle, and/or Last	☐	☐
(18) Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	☐	☐
(19) Student Survey Responses	Student responses to surveys or questionnaires	☐	☐
(20) Student work	Student generated content; writing, pictures, etc.	☐	☐

Category of Data	Elements	Check if Collected by Your System	Check if Requesting from LEA
	Other student work data — Please specify: 	☐	☐
(21) Transcript	Student course grades	☐	☐
	Student course data	☐	☐
	Student course grades/ performance scores	☐	☐
	Other transcript data — Please specify: 	☐	☐
(22) Transportation	Student bus assignment	☐	☐
	Student pick up and/or drop off location	☐	☐
	Student bus card ID number	☐	☐
	Other transportation data — Please specify: 	☐	☐
(23) Other	Please list each additional data element used, stored, or collected by your application: 	☐	☐
(24) None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	☐	☐

EXHIBIT “C” DEFINITIONS

Business Owner (LEA Sponsor): An employee of the LEA with budgetary, legal, or programmatic responsibility sufficient to sponsor the Agreement.

Data Breach: means an incident in which student information that is sensitive, protected, or confidential, as provided by state or federal law, is stolen or is copied, transmitted, viewed, or used by a person unauthorized to engage in that action.

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

Personally Identifiable Information (PII): means information maintained by LEA or Provider that can be used to distinguish, characterize, or trace an individual's identity either directly or indirectly through linkages with other information. *Direct identifiers* include data elements that relate specifically to an individual such as the individual's residence, including for example, name, address, Social Security Number or other identifying number or code, telephone number, e-mail address, or biometric record. *Indirect identifiers* include information that can be combined with other information to identify specific individuals, including, for example, a combination of gender, birth date, geographic indicator, and other descriptors. Other examples of indirect identifiers include place of birth, race, religion, weight, activities, employment information, medical information, education information, and financial information. *Sensitive identifiers* are data elements or types of characterizing information about the subject that could cause special harm or embarrassment to individuals if disclosed. These data do not necessarily need to be removed from datasets shared between LEA and Provider, but they do warrant stronger strategies to mitigate the risk of disclosure. (From <https://studentprivacy.ed.gov/glossary>; NCEE 2022–

004, pages 9–11; and Benschop & Welch ¹, pages 23–25)

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: 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.

¹ Benschop, T. & Welch, M. (n.d.). Statistical disclosure control: A practice guide. Retrieved March 29, 2023 from <https://readthedocs.org/projects/sdcpractice/downloads/pdf/latest/>.

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

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

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

EXHIBIT "D" DIRECTIVE FOR DISPOSITION OF DATA

Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. The terms of the future Disposition are set forth below:

1. Extent of Disposition [Select One]

- ☐ Disposition will be Partial. The categories of data to be disposed of are set forth below or are found in an attachment to this Directive:

- ☒ Disposition will be Complete. Disposition extends to all categories of data.

2. Nature of Disposition [Select One]

- ☒ 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 [Select One]

Data shall be disposed of by the following date:

- ☐ As soon as commercially practicable, consistent with FERPA requirements
- ☒ By no more than 90 days after the conclusion of the services

4. LEA Agrees to Directive

Authorized Representative of LEA

Date of Directive

5. Verification of Disposition of Data [To Be Signed After Disposition]

Authorized Representative of Provider

Date of Disposition

EXHIBIT "E" GENERAL OFFER OF PRIVACY TERMS**1. Offer of Terms by to Subscribing LEA**

Provider offers the same privacy protections found in this DPA between it and Houston Independent School District ("Originating LEA") which is dated [>], to any other LEA ("Subscribing LEA") who accepts this General Offer of Privacy Terms ("General Offer") through its signature below. This General Offer shall extend only to privacy protections, and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the Subscribing LEA may also agree to change the data provided by Subscribing LEA to the Provider to suit the unique needs of the Subscribing LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statutes; (2) a material change in the services and products listed in the originating Service Agreement; or three (3) years after the date of Provider's signature to this Form.

Subscribing LEAs should send the signed **Exhibit "E"** to Provider at the following email address: Tanya Pridgeon, tpridgeo@houstonisd.org.

BY: Date: Printed Name: Title/Position: **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 Houston 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 SUBSCRIBING LEA:

Name: _____

Title: _____

Address: _____

Telephone: _____

Email: _____

EXHIBIT “F” DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks

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.

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 identified below.

Cybersecurity Frameworks

National Institute of Standards and Technology (NIST)

2/24/2020

Check At Least One Box Below

	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 <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf> 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

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 Houston Independent School District (the “Local Education Agency” or “LEA”) and (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

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

1. Duly Authorized School Official with Legitimate Educational Interest

1A. Authorized School Official

The LEA has authorized Provider as a School Official in Exhibit G. Any disclosure of Personally Identifiable Information, data collection, or data analysis under this Agreement is authorized only under the *School Official* exception to the Family Educational Rights and Privacy Act (“**FERPA**”) at 34 CFR § 99.31(a)(1)(B).

1B. Use of Data for Professional Responsibilities, Not Product Development or Research

The purpose for which Student Data are disclosed to the Provider is exclusively to implement the Provider’s professional responsibilities in support of the “Services” described in Exhibit “A”.

Any other use of LEA Data is prohibited except as described in Article IV Section 5 “De-Identified Data”.

Use of data or publication of any subsequent data shared under this agreement for “Research” is not authorized under this agreement other than as described in Exhibit “A”.

If the “Services” evolve, branch, or change to be also or additionally exempt under the *Studies* or *Audit and Evaluation* exceptions, the Provider will be subject to additional policies and Agreements regarding the collection, deidentification, use and publication, and destruction of LEA Records.

Failure by the Provider or Business Owner to report relevant changes in the use of LEA data disclosed under this Agreement to the designated representative for the LEA may result in termination of this Agreement by the LEA.

1C. Specific Data Elements

Both parties affirm that it is a best practice for student data privacy to share the minimum number of education records and fewest data elements necessary to implement Exhibit “A”.

The LEA will exercise good faith in advising the Provider on the availability, appropriateness, and quality of the specific data elements identified by the Provider in Exhibit “B”.

The Provider acknowledges that checking a specific data element in Exhibit “B” does not guarantee either (1) the availability of that specific data element to the Provider, or (2) that the LEA can provide the data element on the Provider’s preferred timetable.

Suggested Attachment: To expedite the review of this DSA and each data element named in Exhibit B as requested from the District, it is suggested that the Provider justify briefly in writing why each specific data element is required to fulfill their professional roles responsibilities of this Project outlined in Exhibit A, and how each data element will be used internally by the Provider.

2. Responsibilities as School Official of Houston ISD

2A. Ethics and Compliance

The individual signing below has authority to enter into this Agreement on behalf of Provider.

Provider acknowledges that the Agreement may be canceled if any conflict of interest or appearance of a conflict of interest is discovered by HISD.

The Provider understands that all Providers who may or will have direct contact with students and continuing duties in connection with the “Services” **must** be fingerprinted. All employees/ subcontractors requiring to be fingerprinted should not perform services in connection with this Project until HISD has reviewed their criminal history background and cleared them to perform services.

Required Attachment: Provider has completed the included Criminal History Background Check Form. The purpose of this form is for vendors to document *whether* their engagement with Houston ISD under this project/contract will involve direct contact with students, as defined within the form. ☒ Yes

The Provider attests that information about fingerprinting requirements (included) has been provided to all employees and/or subcontractors' employees so that they may schedule an appointment to be fingerprinted. Data will not be shared until HISD E&C attests all relevant persons have completed fingerprinting. ☒ Yes ☐ NA

2B. Cybersecurity, File Transfer Mechanisms, and SOC2 Audit Documentation

The Provider agrees to meet the specific minimum technical requirements for data sharing to ensure all data is transferred via a secure mechanism, as determined by HISD IT Operations or another designee of the HISD Superintendent.

LEA data may not be transferred by email under any circumstances.

As Needed: The Provider has detailed any exclusions, variations, or exemptions to the Cybersecurity Framework identified in Exhibit “F”. ☐ Yes ☐ No ☐ NA

The Provider has included their most recent SOC2 Audit. ☐ Yes ☐ No ☐ NA

The Provider has included in writing their specific plans and timeframes to remedy any issues raised in SOC2 audit documentation. ☐ Yes ☐ No ☐ NA

2C. State Regulations for School Officials Regarding Document Retention

Both parties affirm that School Officials support the LEA Business Owner in complying with records retention regulations for Services delivered under Exhibit “A”. Local Schedule GR *Retention Schedule for Records Common to All Local Governments* (13 TAC §7.125(a)(1)) and Local Schedule SD *Retention Schedule for Records of Public School Districts* (13 TAC §7.125(a)(6)) were adopted by the LEA effective April 17, 2016, and September 1, 2019 respectively, and are maintained by HISD Records and Information Management.

Pursuant to **Local Schedule GR1000-41** “Reports and Studies (Non-Fiscal)”, the Provider

attests that, if requested, they will deliver to the LEA a digital *retention copy* of all “working papers, and raw data files” for “special reports or studies” delivered under Exhibit “A”.

Pursuant to **Local Schedule GR1025-08**, the Provider attests that if requested, they will deliver to the LEA a digital *retention copy* of all financial and programmatic records produced under Exhibit “A”, including supporting documents, statistical and program evaluation reports, and other records pertinent to projects or programs funded by state and private grants, through subgrants from the Texas Education Agency, or directly by the U.S. Department of Education. See Local Schedule GR *Part 2(b) GRANT OR LOAN RECORDS*.

A 5-year retention period for many records is necessary to satisfy these requirements adequately. See Local Schedule SD *RETENTION NOTES (b) GRANT RECORDS* (page 8).

2D. School Officials and Indemnification

The Provider shall hold HISD and its past and present and future trustees, officers and employees harmless and shall indemnify all such parties against any and all claims, demands, and causes of action of whatever kind or nature asserted by any third party, occurring or in any way incident to, arising out of, or in connection with any acts of the Provider and its agents, employees, and subcontractors done in connection with this DSA.

Nothing in this DSA shall be construed to create a claim or cause of action against the LEA for which it is not otherwise liable, nor to waive any immunity or defense to which the LEA may be entitled nor to create an impermissible deficiency debt of the LEA.

**HOUSTON INDEPENDENT SCHOOL DISTRICT
CONTRACTOR CRIMINAL HISTORY BACKGROUND CHECK CERTIFICATION**

HISD Contract/Project # 27-09-07 Project Title:
Vendor Name (Prime Contractor):

SECTION I: This section to be completed by all vendors to specify whether their engagement with HISD will involve direct contact with students.

- ☐ **NO direct contact with students** - As required by HISD and applicable law, I hereby certify that **NO employee and/or subcontractor** will have direct contact with any student at HISD as defined under 19 Tex. Admin. Code § 153.1101(7). *Skip Section II and complete Section III below.*
- ☐ **WITH direct contact with students AND continuing duties** - As required by HISD and applicable law, I hereby certify that **the list of employees and/or subcontractors below MAY/WILL** have both direct contact with students and continuing duties at HISD as defined under 19 Tex. Admin. Code 153.1101(7) & (2). *Complete Section II and Section III below. Only entities meeting both criteria are considered as having direct contact with students.*
- 19 Texas Administrative Code 153.1101(7) **Direct contact with students**--The contact that results from activities that provide substantial opportunity for verbal or physical interaction with students that is not supervised by a certified educator or other professional district employee. Contact with students that results from services that do not provide substantial opportunity for unsupervised interaction with a student or students, such as addressing an assembly, officiating a sports contest, or judging an extracurricular event, is not, by itself, direct contact with students. However, direct contact with students does result from any activity that provides substantial opportunity for unsupervised contact with students, which might include, without limitation, the provision of coaching, tutoring, or other services to students.
 - 19 Texas Administrative Code 153.1101(2) **Continuing Duties related to contracted services**—Work duties that are performed pursuant to a contract to provide services to a school entity on a regular, repeated basis rather than infrequently or one-time only.

SECTION II: This section to be completed **ONLY** if vendor's employees/subcontractors will have direct contact with students and continuing duties.

	For each Person, complete: - Full Name as appears on License, - Role/affiliation with Primary Entity, and - Driver's License Number	Person's Date of Birth and Issuing State of DL	Has Person ever been fingerprinted by any <u>public</u> school district in Texas? If YES , provide the name of the school district. If NO or DON'T KNOW , employee must be fingerprinted prior to performing services at HISD.	HISD Internal Use Only
1	Select: ☐ Subcontractor/ Independent ☐ Employee Full Name: <u></u> Driver's License: <u></u>	<u></u> <u></u>	☐ Yes. If yes, name of ISD: <u></u> ☐ No / Don't Know / Cannot Confirm	☐ Approved ☐ Denied
2	Select: ☐ Subcontractor/ Independent ☐ Employee Full Name: <u></u> Driver's License: <u></u>	<u></u> <u></u>	☐ Yes. If yes, name of ISD: <u></u> ☐ No / Don't Know / Cannot Confirm	☐ Approved ☐ Denied
3	Select: ☐ Subcontractor/ Independent ☐ Employee Full Name: <u></u> Driver's License: <u></u>	<u></u> <u></u>	☐ Yes. If yes, name of ISD: <u></u> ☐ No / Don't Know / Cannot Confirm	☐ Approved ☐ Denied
4	Select: ☐ Subcontractor/ Independent ☐ Employee Full Name: <u></u> Driver's License: <u></u>	<u></u> <u></u>	☐ Yes. If yes, name of ISD: <u></u> ☐ No / Don't Know / Cannot Confirm	☐ Approved ☐ Denied
5	Select: ☐ Subcontractor/ Independent ☐ Employee Full Name: <u></u> Driver's License: <u></u>	<u></u> <u></u>	☐ Yes. If yes, name of ISD: <u></u> ☐ No / Don't Know / Cannot Confirm	☐ Approved ☐ Denied

SECTION III – Vendor Certification:

***Attach additional pages as necessary**

By signing below, Vendor acknowledges and agrees that Vendor has obtained the authorization of each above-listed employee for HISD to obtain and review the employee's personal criminal history records to assist with determining the employee's eligibility to provide services at HISD in connection with Vendor's contract with HISD.

Signature of Authorized Representative Date Name & Title of Authorized Representative Taxpayer Identification Number



IdentoGO
By MorphoTrust USA

Local Education Entities

Texas Fingerprint Service Code Form

Service Name: Local Education Entities - Houston ISD

To schedule your ten-minute fingerprint appointment, simply visit
<https://uenroll.identogo.com> and enter the following Service Code

11FJ5N

When prompted, please provide or enter the following Agency Number

TX922040Z

Background Check Waiver

I certify that all information I provided in relation to this criminal history record check is true and accurate. I authorize the Texas Department of Public Safety (DPS) to access Texas and Federal criminal history record information that pertains to me and disseminate that information to the designated Authorized Agency or Qualified Entity with which I am or am seeking to be employed or to serve as a volunteer, through the DPS Fingerprint-based Applicant Clearinghouse of Texas and as authorized by Texas Government Code Chapter 411 and any other applicable state or federal statute or policy.

I authorize the Texas Department of Public Safety to submit my fingerprints and other application information to the FBI for the purpose of comparing the submitted information to available records in order to identify other information that may be pertinent to the application. I authorize the FBI to disclose potentially pertinent information to the DPS during the processing of this application and for as long hereafter as may be relevant to the activity for which this application is being submitted. I understand that the FBI may also retain my fingerprints and other applicant information in the FBI's permanent collection of fingerprints and related information, where all such data will be subject to comparisons against other submissions received by the FBI and to further disseminations by the FBI as may be authorized under the Privacy Act of 1974 (5 USC 552a). I understand my fingerprints will be searched by and against civil, criminal and latent fingerprints in the Next Generation Identification (NGI) system. I understand I am entitled to obtain a copy of any criminal history record check and challenge the accuracy and completeness of the information before a final determination is made by the Qualified Entity. I also understand the Qualified Entity may deny me access to children, the elderly, or individuals with disabilities until the criminal history record check is completed. If a need arises to challenge the FBI record response, you may contact the agency that submitted the information to the FBI, or you may send a written challenge request to the FBI's Criminal Justice Information Services (CJIS) Division at FBI CJIS Division, Attention: Correspondence Group, 1000 Custer Hollow Road, Clarksburg, WV 26306.



Don't have access to the Internet? You can still schedule an appointment by calling 888.467.2080