

DATA PRIVACY AGREEMENT (DPA)
FOR TEXAS K-12 INSTITUTIONS

LEA NAME [Box 1]

DATE [Box 2]

and

OPERATOR NAME [Box 3]

DATE [Box 4]

Background and Instructions

History of Agreement- This agreement has been drafted by the Texas Student Privacy Alliance (TXSPA). The Alliance is a collaborative group of Texas school districts that share common concerns around student and data privacy. The Texas K-12 CTO Council is the organization that sponsors the TXSPA and the TXSPA is the Texas affiliate of the national Student Data Privacy Consortium (SDPC). The SDPC works with other state alliances by helping establish common data privacy agreements unique to the jurisdiction of each state. This Texas agreement was drafted specifically for K-12 education institutions and included broad stakeholder input from Texas school districts, statewide associations such as TASB, TASA, and TASBO, and the Texas Education Agency. The purpose of this agreement is to set standards of both practice and expectations around data privacy such that all parties involved have a common understanding of expectations. This agreement also provides a mechanism (Exhibit E- General Offer of Terms) that would allow an Operator to extend the ability of other Texas school districts to be covered under the terms of the agreement should an Operator sign Exhibit E. This mechanism is intended to create efficiencies for both Operators and LEAs and generally enhance privacy practices and expectations for K-12 institutions and for companies providing services to K-12 institutions.

Instructions for Operators: This agreement is intended to be provided to an Operator from a LEA. The Operator should fully read the agreement and is requested to complete the below areas of the agreement. Once the Operator accepts the terms of the agreement, the Operator should wet sign the agreement and return it to the LEA. Once the LEA signs the agreement, the LEA should provide a signed copy of the agreement to the Operator.

Article/Exhibit	Box #	Description
Cover Page	Box # 3	Official Name of Operator
Cover Page	Box # 4	Date Signed by Operator
Recitals	Box #5	Contract Title for Service Agreement
Recitals	Box #6	Date of Service Agreement
Article 7	Boxes #7-10	Operator's designated representative
Signature Page	Boxes #15-19	Authorized Operator's representative signature
Exhibit A	Box #25	Description of services provided
Exhibit B	All Applicable Boxes	<ul style="list-style-type: none">• Operator notates if data is collected to provide the described services.• Defines the schedule of data required for the Operator to provide the services outlined in Exhibit A
Exhibit D	All Applicable Boxes	(Optional Exhibit): Defines deletion or return of data expectations by LEA

Exhibit E	All Applicable Boxes	(Optional Exhibit): Operator may, by signing the Form of General Offer of Privacy Terms (General Offer, attached as <u>Exhibit E</u>), be bound by the terms of this DPA to any other Subscribing LEA who signs the acceptance in said Exhibit.
Exhibit F	Boxes # 25-29	A list of all Subprocessors used by the Operator to perform functions pursuant to the Service Agreement, list security programs and measures, list Operator's security measures

Instructions for LEA and/or Subscribing LEA: This agreement is intended to be provided to an Operator from a LEA. Upon receiving an executed agreement from an Operator, the LEA should fully review the agreement and if agreeable, should have an authorized LEA contact wet sign the agreement. Once signed by both the Operator and LEA, the LEA should send a copy of the signed agreement to the Operator.

Article/Exhibit	Box #	Description
Cover Page	Box # 1	Official Name of LEA
Cover Page	Box #2	Date Signed by LEA
Article 7	Boxes #11-14	LEA's designated representative
Signature Page	Boxes #20-24	Authorized LEA representative's signature
Exhibit D	All Applicable Boxes	(Optional Exhibit): Defines deletion or return of data expectations by LEA
Exhibit E	All Applicable Boxes	(Optional Exhibit) Only to be completed by a Subscribing LEA

RECITALS

WHEREAS, the Operator has agreed to provide the Local Education Agency (“LEA”) with certain digital educational services (“Services”) according to a contract titled “_____”
[Box 5]
and dated _____ (the “Service Agreement”), and
[Box 6]

WHEREAS, in order to provide the Services described in the Service Agreement, the Operator may

receive or create and the LEA may provide documents or data that are covered by federal statutes, among them, the Federal Educational Rights and Privacy Act (“FERPA”) at 20 U.S.C. 1232g (34 CFR Part 99), Children’s Online Privacy Protection Act (“COPPA”), 15 U.S.C. 6501-6506, and Protection of Pupil Rights Amendment (“PPRA”) 20 U.S.C. 1232h; and

WHEREAS, the documents and data transferred from LEAs and created by the Operator’s Services are also subject to state student privacy laws, including Texas Education Code Chapter 32; and

WHEREAS, the Operator may, by signing the "General Offer of Privacy Terms", agree to allow other LEAs in Texas the opportunity to accept and enjoy the benefits of this DPA for the Services described within, without the need to negotiate terms in a separate DPA.

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

ARTICLE I: PURPOSE AND SCOPE

1. **Nature of Services Provided.** The Operator has agreed to provide digital educational services as outlined in Exhibit A and the Agreement.
2. **Purpose of DPA.** For Operator to provide services to the LEA it may become necessary for the LEA to share certain LEA Data. This DPA describes the Parties’ responsibilities to protect Data.
3. **Data to Be Provided.** In order for the Operator to perform the Services described in the Service Agreement, LEA shall provide the categories of data described in the Schedule of Data, attached as Exhibit B.
4. **DPA Definitions.** The definitions of terms used in this DPA are found in Exhibit C. In the event of a conflict, definitions used in this DPA shall prevail over terms used in the Service Agreement.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Ownership of Data.** All Data transmitted to the Operator pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Operator further acknowledges and agrees that all copies of such Data transmitted to the Operator, 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 Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Data contemplated per the Service Agreement shall remain the exclusive property of the LEA.
2. **Operator Materials.** Operator retains all right, title and interest in and to any and all of Operator's software, materials, tools, forms, documentation, training and implementation materials and intellectual property ("Operator Materials"). Operator grants to the LEA a personal, nonexclusive license to use the Operator Materials for its own non-commercial, incidental use as set forth in the Service Agreement. Operator represents that it has all intellectual property rights necessary to enter into and perform its obligations in this DPA and the Service Agreement, warrants to the District that the District will have use of any intellectual property contemplated by the Service Agreement free and clear of claims of any nature by any third Party including, without limitation, copyright or patent infringement claims, and agrees to indemnify the District for any related claims.
3. **Parent Access.** LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Data on the pupil's records, correct erroneous information, and procedures for the transfer of pupil-generated content to a personal account, consistent with the functionality of services. Operator shall respond in a reasonably timely manner (and no later than 28 days from the date of the request) to the LEA's request for Data in a pupil's records held by the Operator to view or correct as necessary. In the event that a parent of a pupil or other individual contacts the Operator to review any of the Data accessed pursuant to the Services, the Operator shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.
4. **Data Portability.** Operator shall, at the request of the LEA, make Data available including Pupil Generated Content in a readily accessible format.
5. **Third Party Request.** Should a Third Party, including law enforcement or a government entity, contact Operator with a request for data held by the Operator pursuant to the Services, the Operator shall immediately (within 1 business day), and to the extent legally permitted, redirect the Third Party to request the data directly from the LEA, notify the LEA of the request, and provide a copy of the request to the LEA. Furthermore, if legally permissible, Operator shall promptly notify the LEA of a subpoena compelling disclosure to a Third Party and provide a copy of the subpoena with sufficient time for the LEA to raise objections to the subpoena. The Operator will not use, disclose, compile, transfer, or sell the Data and/or any portion thereof to any third party or other entity or allow any other third party or other entity to use, disclose, compile, transfer or sell the Data and/or any portion thereof. Notwithstanding any provision of this DPA or Service Agreement to the contrary, Operator understands that the LEA is subject to and will comply with the Texas Public Information Act (Chapter 552, Texas Government Code). Operator understands and agrees that information, documentation and other material in connection with the DPA and Service Agreement may be subject to public disclosure.
6. **No Unauthorized Use.** Operator shall use Data only for the purpose of fulfilling its duties and obligations under the Service Agreement and will not share Data with or disclose it to any Third Party without the prior written consent of the LEA, except as required by law or to fulfill its duties and obligations under the Service Agreement.
7. **Subprocessors.** All Subprocessors used by the Operator to perform functions pursuant to the Service Agreement shall be identified in Exhibit F. Operator shall either (1) enter into written agreements with all Subprocessors performing functions pursuant to the Service Agreement, such that the Subprocessors agree to protect Data in a manner the same as or better than as provided pursuant to the terms of this DPA, or (2) indemnify and hold harmless the LEA, its officers, agents, and employees from any and all claims, losses, suits, or liability including attorneys' fees for damages or costs resulting from the acts or omissions of its Subprocessors. Operator shall periodically conduct or review compliance monitoring and assessments of Subprocessors to determine their compliance with this DPA. Subprocessors shall agree to the provisions of the DPA regarding governing law, venue, and jurisdiction.

ARTICLE III: DUTIES OF LEA

1. **Provide Data In Compliance With State and Federal Law.** LEA shall provide data for the purposes of the Service Agreement in compliance with FERPA, COPPA, PPRA, Texas Education Code Chapter 32, and all other Texas privacy statutes cited in this DPA as these laws and regulations apply to the contracted services. The LEA shall not be required to provide Data in violation of applicable laws. Operator may not require LEA or users to waive rights under applicable laws in connection with use of the Services.
2. **Consider Operator as School Official.** The Parties agree that Operator is a “school official” under FERPA and has a legitimate educational interest in personally identifiable information from education records. For purposes of the Service Agreement and this DPA, Operator: (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 education records
3. **Reasonable Precautions.** LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted data.
4. **Unauthorized Access Notification.** LEA shall notify Operator promptly of any known unauthorized access. LEA will assist Operator in any efforts by Operator to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF OPERATOR

1. **Privacy Compliance.** Operator may receive Personally Identifiable Information (“PII”) from the District in the course of fulfilling its duties and obligations under the Service Agreement. The Operator shall comply with all applicable State and Federal laws and regulations pertaining to data privacy and security including FERPA, COPPA, PPRA, Texas Education Code Chapter 32, and all other Texas privacy statutes cited in this DPA.
2. **Employee Obligation.** Operator shall require all employees and agents who have access to Data to comply with all applicable provisions of this DPA with respect to the data shared under the Service Agreement. Operator agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Data pursuant to the Service Agreement.
3. **De-identified Information.** De-identified Information may be used by the Operator only for the purposes of development, product improvement, to demonstrate or market product effectiveness, or research as any other member of the public or party would be able to use de-identified data pursuant to 34 CFR 99.31(b). Operator agrees not to attempt to re-identify De-identified Information and not to transfer De-identified Information to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to LEA who has provided prior written consent for such transfer. Operator shall not copy, reproduce or transmit any De-identified Information or other Data obtained under the Service Agreement except as necessary to fulfill the Service Agreement.
4. **Access To, Return, and Disposition of Data.** Upon written request of LEA, Operator shall dispose of or delete all Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained, and transfer said data to LEA or LEA’s designee within sixty (60) days of the date of termination and according to a schedule and procedure as the Parties may reasonably agree. Operator acknowledges LEA’s obligations regarding retention of governmental data, and shall not destroy Data except as permitted by LEA. Nothing in the Service Agreement shall authorize Operator to maintain Data obtained under the Service Agreement beyond the time period reasonably needed to complete the disposition. Disposition shall include (1) the shredding of any hard copies of any Data; (2) Data Destruction; or (3) Otherwise modifying the personal information in those records to make it unreadable or indecipherable. Operator shall provide written notification to LEA when the Data has been disposed of.

The duty to dispose of Data shall not extend to data that has been de-identified or placed in a separate Student account, pursuant to the other terms of the DPA. The LEA may employ a “Request for Return or Deletion of Data” FORM, a sample of this form is attached on Exhibit “D”). Upon receipt of a request from the LEA, the Operator will immediately provide the LEA with any specified portion of the Data within five (5) business days of receipt of said request.

5. **Targeted Advertising Prohibition.** Operator is prohibited from using or selling Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing, advertising, or other commercial efforts by a Operator; (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Service to LEA; or (d) use the Data for the development of commercial products or services, other than as necessary to provide the Service to LEA. This section does not prohibit Operator from generating legitimate personalized learning recommendations.
6. **Access to Data.** Operator shall make Data in the possession of the Operator available to the LEA within five (5) business days of a request by the LEA.

ARTICLE V: DATA PROVISIONS

1. **Data Security.** The Operator agrees to abide by and maintain adequate data security measures, consistent with industry standards and technology best practices, to protect Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of Operator are set forth below. Operator shall further detail its security programs and measures in Exhibit F. These measures shall include, but are not limited to:
 - a. **Passwords and Employee Access.** Operator shall secure usernames, passwords, and any other means of gaining access to the Services or to Data, at a level consistent with an industry standard agreed upon by LEA (e.g. suggested by Article 4.3 of NIST 800-63-3). Operator shall only provide access to Data to employees or subprocessors that are performing the Services. Employees with access to Data shall have signed confidentiality agreements regarding said Data. All employees with access to Data shall pass criminal background checks.
 - b. **Security Protocols.** Both parties agree to maintain security protocols that meet industry best practices in the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. Operator shall maintain all data obtained or generated pursuant to the Service Agreement in a secure computer environment.
 - c. **Employee Training.** The Operator shall provide periodic security training to those of its employees who operate or have access to the system.
 - d. **Security Technology.** When the Services are accessed using a supported web browser, Secure Socket Layer (“SSL”) or equivalent technology shall be employed to protect data from unauthorized access. The service security measures shall include server authentication and data encryption. Operator shall host data pursuant to the Service Agreement in an environment using a firewall that is periodically updated according to industry standards.
 - e. **Security Contact.** Operator shall provide the name and contact information of Operator's Security Contact on Exhibit F. The LEA may direct security concerns or questions to the Security Contact.
 - f. **Periodic Risk Assessment.** Operator shall conduct periodic risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner. Upon request, Operator will provide the LEA an executive summary of the risk assessment or equivalent report and confirmation of remediation.

g. Backups. Operator agrees to maintain backup copies, backed up at least daily, of Data in case of Operator's system failure or any other unforeseen event resulting in loss of any portion of Data.

h. Audits. Within 30 days of receiving a request from the LEA, and not to exceed one request per year, the LEA may audit the measures outlined in the DPA. The Operator will cooperate fully with the LEA and any local, state, or federal agency with oversight authority/jurisdiction in connection with any audit or investigation of the Operator and/or delivery of Services to students and/or LEA, and shall provide full access to the Operator's facilities, staff, agents and LEA's Data and all records pertaining to the Operator, LEA and delivery of Services to the Operator. Failure to cooperate shall be deemed a material breach of the DPA. The LEA may request an additional audit if a material concern is identified.

i. Incident Response. Operator shall 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 any portion of Data, including PII, and agrees to provide LEA, upon request, an executive summary of the written incident response plan.

2. Data Breach. When Operator reasonably suspects and/or becomes aware of an unauthorized disclosure or security breach concerning any Data covered by this Agreement, Operator shall notify the District within 24 hours. The Operator shall take immediate steps to limit and mitigate the damage of such security breach to the greatest extent possible. If the incident involves criminal intent, then the Operator will follow direction from the Law Enforcement Agencies involved in the case.

a. The security breach notification to the LEA shall be written in plain language, and address the following

1. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
2. A description of the circumstances surrounding the disclosure or breach, including the actual or estimated, time and date of the breach, and Whether the notification was delayed as a result of a law enforcement investigation.

b. Operator agrees to adhere to all requirements in applicable state and federal law with respect to a Data breach or disclosure, including any required responsibilities and procedures for notification or mitigation

c. In the event of a breach or unauthorized disclosure, the Operator shall cooperate fully with the LEA, including, but not limited to providing appropriate notification to individuals impacted by the breach or disclosure. Operator will reimburse the LEA in full for all costs incurred by the LEA in investigation and remediation of any Security Breach caused in whole or in part by Operator or Operator's subprocessors, including but not limited to costs of providing notification and providing one year's credit monitoring to affected individuals if PII exposed during the breach could be used to commit financial identity theft.

d. The LEA may immediately terminate the Service Agreement if the LEA determines the Operator has breached a material term of this DPA.

e. The Operator's obligations under Section 7 shall survive termination of this DPA and Service Agreement until all Data has been returned and/or Securely Destroyed.

ARTICLE VI- GENERAL OFFER OF PRIVACYTERMS

1. **General Offer of Privacy Terms.** Operator may, by signing the attached Form of General Offer of Privacy Terms (General Offer, attached as Exhibit E), be bound by the terms of this DPA to any other LEA who signs the acceptance in said Exhibit.

ARTICLE VII: MISCELLANEOUS

1. **Term.** The Operator shall be bound by this DPA for the duration of the Service Agreement or so long as the Operator maintains any Data. Notwithstanding the foregoing, Operator agrees to be bound by the terms and obligations of this DPA for no less than three (3) years.
2. **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.
3. **Effect of Termination Survival.** If the Service Agreement is terminated, the Operator shall dispose of all of LEA's Data pursuant to Article IV, section 5.
4. **Priority of Agreements.** This DPA shall govern the treatment of Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes cited in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, or with any other bid/RFP, license agreement, terms of service, privacy policy, or other writing, the terms of this DPA shall apply and take precedence. Except as described in this paragraph, all other provisions of the Service Agreement shall remain in effect.
5. **Notice.** All notices or other communication required or permitted to be given hereunder must be in writing and given by personal delivery, facsimile or e-mail transmission (if contact information is provided for the specific mode of delivery), or first-class mail, postage prepaid, sent to the designated representatives before: The designated representative for the Operator for this Agreement is:

First Name:	_____	[Box 7]
Last Name:	_____	[Box 8]
Operator's Company Name:	_____	[Box 9]
Title of Representative:	_____	[Box 10]

The designated representative for the LEA for this Agreement is:

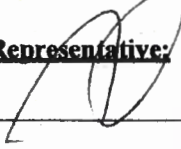
First Name:	_____	[Box 11]
Last Name:	_____	[Box 12]
LEA's Name:	_____	[Box 13]
Title of Representative:	_____	[Box 14]

6. **Entire Agreement.** This DPA constitutes the entire agreement of the parties relating to the subject matter and supersedes all prior communications, representations, or agreements, oral or written, by the Parties. 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.
7. **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.
8. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF TEXAS, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY IN WHICH THIS AGREEMENT IS FORMED FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS SERVICE AGREEMENT OR THE TRANSACTIONS CONTEMPLATED HEREBY.
9. **Authority.** Operator represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Data and/or any portion thereof, or may own, lease or control equipment or facilities of any kind where the Data and portion thereof is stored, maintained or used in any way.
10. **Waiver.** Waiver by any party to this DPA of any breach of any provision of this DPA or warranty of representation set forth herein shall not be construed as a waiver of any subsequent breach of the same or any other provision. The failure to exercise any right under this DPA shall not operate as a waiver of such right. All rights and remedies provided for in this DPA are cumulative. Nothing in this DPA shall be construed as a waiver or relinquishment of any governmental immunities or defenses on behalf of the LEA, its trustees, officers, employees, and agents as a result of the execution of this DPA or performance of the functions or obligations described herein.
11. **Assignment.** The Parties may not assign their rights, duties, or obligations under this DPA, either in whole or in part, without the prior written consent of the other Party except that either party may assign any of its rights and obligations under this DPA without consent in connection with any merger (including without limitation by operation of law), consolidation, reorganization, or sale of all or substantially all of its related assets or similar transaction. This DPA inures to the benefit of and shall be binding on the Parties' permitted assignees, transferees and successors.

[Signature Page Follows]

IN WITNESS WHEREOF, the parties have executed this DATA PRIVACY AGREEMENT FOR TEXAS K-12 INSTITUTIONS as of the last day noted below.

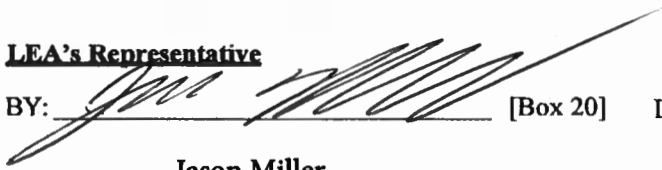
Operator's Representative:

BY:  [Box 15] Date: 11/19/20 [Box 16]

Printed Name: Adam Dean [Box 17] Title/Position: VP of Finance [Box 18]

Address for Notice Purposes: contracts@k12insight.com [Box 19]

LEA's Representative

BY:  [Box 20] Date: 11-19-2020 [Box 21]

Printed Name: Jason Miller [Box 22] Title/Position: CFO [Box 23]

Address for Notice Purposes: 315 W. West Dr, Leander, TX 78641 [Box 24]

Note: Electronic signature not permitted.

EXHIBIT “A”

DESCRIPTION OF SERVICES

Description : [Box 25]

EXHIBIT “ B”

SCHEDULE OF DATA

Instructions: Operator should identify if LEA data is collected to provide the described services. If LEA data is collected to provide the described services, check the boxes indicating the data type collected. If there is data collected that is not listed, use the “Other” category to list the data collected.

- ☐ We do not collect LEA Data to provide the described services.
- ☐ We do collect LEA Data to provide the described services.

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.	<input type="checkbox"/>
	Other application technology meta data-Please specify:	<input type="checkbox"/>
Application Use Statistics	Meta data on user interaction with application- Please specify:	<input type="checkbox"/>
Assessment	Standardized test scores	<input type="checkbox"/>
	Observation data	<input type="checkbox"/>
	Other assessment data-Please specify:	<input type="checkbox"/>
Attendance	Student school (daily) attendance data	<input type="checkbox"/>
	Student class attendance data	<input type="checkbox"/>
Communications	Online communications that are captured (emails, blog entries)	<input type="checkbox"/>
Conduct	Conduct or behavioral data	<input type="checkbox"/>
	Date of Birth	<input type="checkbox"/>

	Demographics	Place of Birth	<input type="checkbox"/>	
		Gender	<input type="checkbox"/>	
		Ethnicity or race	<input type="checkbox"/>	
		Language information (native, preferred or primary language spoken by student)	<input type="checkbox"/>	
		Other demographic information-Please specify:	<input type="checkbox"/>	
	Enrollment	Student school enrollment	<input type="checkbox"/>	
		Student grade level	<input type="checkbox"/>	
		Homeroom	<input type="checkbox"/>	
		Guidance counselor	<input type="checkbox"/>	
		Specific curriculum programs	<input type="checkbox"/>	
		Year of graduation	<input type="checkbox"/>	
		Other enrollment information-Please specify:	<input type="checkbox"/>	
	Parent/Guardian Contact Information	Address	<input type="checkbox"/>	
		Email	<input type="checkbox"/>	
		Phone	<input type="checkbox"/>	
	Parent/Guardian ID	Parent ID number (created to link parents to students)	<input type="checkbox"/>	
	Parent/Guardian Name	First and/or Last	<input type="checkbox"/>	
	Schedule	Student scheduled courses	<input type="checkbox"/>	
		Teacher names	<input type="checkbox"/>	
Special Indicator	English language learner information	<input type="checkbox"/>		
	Low income status	<input type="checkbox"/>		
	Medical alerts /health data	<input type="checkbox"/>		
	Student disability information	<input type="checkbox"/>		
	Specialized education services (IEP or 504)	<input type="checkbox"/>		
	Living situations (homeless/foster care)	<input type="checkbox"/>		
	Other indicator information-Please specify:	<input type="checkbox"/>		

Category of Data	Elements	Check if used by your system
Student Contact Information	Address	<input type="checkbox"/>
	Email	<input type="checkbox"/>
	Phone	<input type="checkbox"/>
Student Identifiers	Local (School district) ID number	<input type="checkbox"/>
	State ID number	<input type="checkbox"/>
	Vendor/App assigned student ID number	<input type="checkbox"/>
	Student app username	<input type="checkbox"/>
	Student app passwords	<input type="checkbox"/>
Student Name	First and/or Last	<input type="checkbox"/>
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	<input type="checkbox"/>
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	<input type="checkbox"/>
Student Survey Responses	Student responses to surveys or questionnaires	<input type="checkbox"/>
Student work	Student generated content; writing, pictures etc.	<input type="checkbox"/>
	Other student work data -Please specify:	<input type="checkbox"/>
Transcript	Student course grades	<input type="checkbox"/>
	Student course data	<input type="checkbox"/>
	Student course grades/performance scores	<input type="checkbox"/>
	Other transcript data -Please specify:	<input type="checkbox"/>
	Student bus assignment	<input type="checkbox"/>
	Student pick up and/or drop off location	<input type="checkbox"/>

	Transportation	Student bus card ID number	<input type="checkbox"/>
		Other transportation data -Please specify:	<input type="checkbox"/>
	Other	Please list each additional data element used, stored or collected through the services defined in Exhibit A	<input type="checkbox"/>

EXHIBIT “C”

DEFINITIONS

HB 2087: The statutory designation for what is now Texas Education Code Chapter 32 relating to pupil records.

Data: Data shall include, but is not limited to, the following: student data, educational records, employee data, metadata, user content, course content, materials, and any and all data and information that the District (or any authorized end user(s)) uploads or enters through their use of the product. Data also specifically includes all personally identifiable information in education records, directory data, and other non-public information for the purposes of Texas and Federal laws and regulations. Data as specified in Exhibit B is confirmed to be collected or processed by the Operator pursuant to the Services. Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student’s use of Operator’s services.

De-Identified Information (DII): De-Identified Information is Data subjected to a process by which any Personally Identifiable Information (“PII”) is removed or obscured in a way that eliminates the risk of disclosure of the identity of the individual or information about them, and cannot be reasonably re-identified.

Data Destruction: Provider shall certify to the District in writing that all copies of the Data stored in any manner by Provider have been returned to the District and permanently erased or destroyed using industry best practices to assure complete and permanent erasure or destruction. These industry best practices include, but are not limited to, ensuring that all files are completely overwritten and are unrecoverable. Industry best practices do not include simple file deletions or media high level formatting operations.

NIST 800-63-3: Draft National Institute of Standards and Technology (“NIST”) Special Publication 800-63-3 Digital Authentication Guideline.

Personally Identifiable Information (PII): The terms “Personally Identifiable Information” or “PII” shall include, but are not limited to, Data, metadata, and user or pupil-generated content obtained by reason of the use of Operator’s software, website, service, or app, including mobile apps, whether gathered by Operator or provided by LEA or its users, students, or students’ parents/guardians. PII includes Indirect Identifiers, which is any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty. For purposes of this DPA, Personally Identifiable Information shall include the categories of information listed in the definition of Data.

Pupil-Generated Content: The term “pupil-generated content” means materials or content created by a pupil during and for the purpose of education including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of pupil content.

Subscribing LEA: A LEA that was not party to the original Services Agreement and who accepts the Operator’s General Offer of Privacy Terms.

Subprocessor: For the purposes of this Agreement, the term “Subprocessor” (sometimes referred to as the “Subcontractor”) means a party other than LEA or Operator, who Operator uses for data collection, analytics, storage, or other service to operate and/or improve its software, and who has access to PII.

Targeted Advertising: Targeted advertising means presenting an advertisement to a student where the selection of the advertisement is based on student information, student records or student generated content or inferred over time from the usage of the Operator’s website, online service or mobile application by such student or the retention of such student’s online activities or requests over time.

Texas Student Privacy Alliance: The Texas Student Privacy Alliance (TXSPA) is a collaborative group of Texas school districts that share common concerns around student privacy. The goal of the TXSPA is to set standards of both practice and expectations around student privacy such that all parties involved have a common understanding of expectations. The Texas K-12 CTO Council is the organization that sponsors TXSPA and the TXSPA is the Texas affiliate of the National Student Privacy Consortium.

EXHIBIT “D”

SAMPLE REQUEST FOR RETURN OR DELETION OF DATA

Instructions: This Exhibit is optional and provided as a sample ONLY. It is intended to provide a LEA an example of what could be used to request a return or deletion of data.

_____ directs _____ to
LEA OPERATOR

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

1. Extent of Return or Disposition

☐

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

☐

Return or Disposition is Complete. Disposition extends to all categories of data.

2. Nature of Return or Disposition

☐

Disposition shall be by destruction or deletion of data.

☐

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

3. Timing of Return or Disposition

Data shall be returned or disposed of by the following date:

☐

As soon as commercially practicable

☐

By the following agreed upon date:

4. Signatures

Authorized Representative of LEA

Date:

5. Verification of Disposition of Data

Authorized Representative of Operator

Date:

EXHIBIT " E"

GENERAL OFFER OF PRIVACY TERMS

Instructions: This is an optional Exhibit in which the Operator may, by signing this Exhibit, be bound by the terms of this DPA to any other Subscribing LEAs who sign the acceptance in said Exhibit. The originating LEA SHOULD NOT sign this Exhibit, but should make Exhibit E, if signed by an Operator, readily available to other Texas K-12 institutions through the TXSPA web portal. Should a Subscribing LEA, after signing a separate Service Agreement with Operator, want to accept the General Offer of Terms, the Subscribing LEA should counter-sign the Exhibit E and notify the Operator that the General Offer of Terms have been accepted by a Subscribing LEA.

1. Offer of Terms

Operator offers the same privacy protections found in this DPA between it and

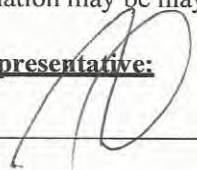
Leander Independent School District

and which is dated [05/27/20] to any other LEA ("Subscribing LEA") who accepts this General Offer through its signature below. This General Offer shall extend only to privacy protections and Operator's signature shall not necessarily bind Operator to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Operator and the other LEA may also agree to change the data provided by LEA to the Operator to suit the unique needs of the LEA. The Operator 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;
- (3) the expiration of three years after the date of Operator's signature to this Form.

Operator shall notify the Texas Student Privacy Alliance (TXSPA) in the event of any withdrawal so that this information may be may be transmitted to the Alliance's users.

Operator's Representative:

BY:  _____

Date: 11/19/20

Printed Name: Adam Dean

Title/Position: VP of Finance

2. Subscribing LEA

A Subscribing LEA, by signing a separate Service Agreement with Operator, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and Operator shall therefore be bound by the same terms of this DPA. The Subscribing LEA, also by its signature below, agrees to notify Operator that it has accepted this General Offer, and that such General Offer is not effective until Operator has received said notification.

Subscribing LEA's Representative:

BY: _____

Date: _____

Printed Name: _____

Title/Position: _____

EXHIBIT “F”

DATA SECURITY

1. **Operator’s Security Contact Information:**

_____ [Box 26]
Named Security Contact

_____ [Box 27]
Email of Security Contact

_____ [Box 28]
Phone Number of Security Contact

2. **List of Operator’s Subprocessors:**

[Box 29]

3. **Additional Data Security Measures:**

[Box 30]



K-12 SOLUTIONS FOR CUSTOMER SERVICE
AND
SUSTAINED STAKEHOLDER ENGAGEMENT

SALES ORDER FORM

K12 *Insight* LLC

2291 Wood Oak Drive, Suite 300
Herndon, VA 20171

Sarah Berman
Strategic Account Executive

Tel: 703-542-9633
Fax: 703-935-1403

sberman@k12insight.com
www.k12insight.com

CLIENT INFORMATION			
Name	Leander Independent School District – TX		
Address	P.O. Box 218		
City, State Zip	Leander, Texas 78646		
Proposal Date	04/24/2020	Student Enrollment	39,028

DATES AND TERM OF INITIAL CONTRACT			
Term	Start Date	End Date	Total
Year 1	9/1/2020	8/31/2021	\$87,570

The pricing and terms in this proposal are valid for 30 days from proposal date.

LET'S TALK! CUSTOMER EXPERIENCE PLATFORM SERVICES	Standard Price
<input checked="" type="checkbox"/> SUBSCRIPTION TO LET'S TALK! PLATFORM <p>K12 <i>Insight</i> provides Software as a Service to serve as a single, centralized, secure cloud-based repository of all incoming questions, comments, concerns, suggestions and compliments by any stakeholder in the district. Software customization is offered for multiple languages.</p> <p>Also includes mobile app and customization of Let's Talk! platform to automatically assign ownership of all dialogues from multiple channels and issue alerts to administrators. Administrators will be able to access the Let's Talk! system using a secure login ID and password, allowing them to collaborate with each other and respond to incoming dialogue.</p> <p>Subscription includes continuous and ongoing support via a dedicated Let's Talk! customer service team and access to dedicated engagement specialists to assist in feedback management and implementation.</p>	<p>\$3.50 per student, per year</p>

YEAR ONE SERVICES 09/01/2020 to 08/31/2021					
Let's Talk! Platform Services					
Quantity	Service	Price	Discounted Price	Unit	Cost
1	Subscription to Let's Talk! Platform	\$3.50	\$2.50	per student, per year	\$97,570
SUBTOTAL for Let's Talk! Platform Services					\$97,570
Legacy Discount Applied					(\$10,000)
TOTAL for Let's Talk! Platform Services					\$87,570

BILLING CONTACT

Name	Corey Ryan		
Title	Chief Communications Officer		
Email	Corey.Ryan@leanderisd.org		
Phone	512-570-0000	Fax	512-570-0035

ORDER CONFIRMATION

This Sales Order Form is subject to and governed by the Terms of Service (v1.20) located here: www.k12insight.com/terms-of-service/1.20, and any addenda attached. No other terms apply to K12 *Insight's* services, unless attached herein and agreed to. Client has received, read, and understood all terms applicable to K12 *Insight's* services, attached. Where applicable, Client has pre-audited this Order in the manner required by all applicable state and local laws. Client representative below hereby represents to have the authority to engage these services on behalf of Client.

AUTHORIZED SIGNATURES

Executed for and on behalf of the Client by:

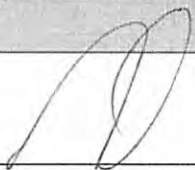
Client Signature

Elaine Cogburn Digitally signed by Elaine Cogburn
Date: 2020.05.27 08:31:54 -05'00'

Name	Elaine Cogburn	Date	05.27.2020
Title	Chief Financial Officer	Email	Elaine.Cogburn@leanderisd.org
Phone	512-570-0405	Fax	

For and on behalf of K12 *Insight* LLC, a division of Zarca Interactive, by:

K12 Insight Signature

			
Name	Adam Dean	Date	8/31/20
Title	VP of Finance		

K12 INSIGHT INTERNAL USE ONLY

Prepared	Lori Ingram 04/24/2020	Reviewed	Sarah Berman 04/24/2020	Approved	Krista Coleman 04/24/2020
-----------------	---------------------------	-----------------	----------------------------	-----------------	------------------------------

K12 *Insight* PRIVACY POLICY

K12 *Insight*, LLC (“**K12 *Insight*”** “us” or “we”) is committed to protecting the personal information of our Clients, users, and visitors. This Privacy Policy explains how your personal information is collected, used, and disclosed by K12 *Insight* in connection with our website and online services available at www.k12insight.com, or any other website or mobile application linked to this Privacy Policy (collectively, the “**Sites**”). This Privacy Policy also describes how we collect Data through the online software platform and technology services solutions used by our Clients to engage with their customers, end users, students, parents, school community members, and other individuals (the “**Client Solutions**”). The Site and Client Solutions together are collectively referred to as our “**Service.**” “**You**” or “**your**” means a visitor or a user (whether signed in or not) of our Service.

This Privacy Policy describes K12 *Insight*’s use of information collected through the Service. This Privacy Policy does not govern the data practices of any third parties, such as our Clients who may use your personal information collected through the Service for their own purposes in accordance with their own privacy policy.

By accessing or using our Service, you signify that you have read, understood, and agree to our collection, storage, use and disclosure of personal information as described in this Privacy Policy.

1. OUR SOLUTION, SOFTWARE AND SERVICES

K12 *Insight* software solutions are provided in an Application Service Provider (“ASP”) model and accessed using industry-standard web browsers via the web, or a mobile device, or using a mobile app on a mobile device. Many of our Clients use our software solutions on a Self-Service basis, whereby the Client or its authorized staff are solely responsible for the data they input to our system and the data our systems collect from their stakeholders. Such use of our solution is referred to in this document as “Self-Service.” In some instances, we may manage a project on behalf of our Clients, which we refer to as our “Consulting Service.” In either scenario, we process Client Data (defined below) on our Client’s behalf.

2. HOW WE COLLECT INFORMATION AND DATA

We collect personal information in a variety of ways through our Sites and Solutions.

When registering for our Services or submitting a request on our Sites, we generally request the following information: including, but not limited to, name and contact information, company name, name of business representative, title of business representatives, company address, telephone number, email address, username and password, and billing information which may include credit card numbers. Clients also provide us with information regarding the services they have ordered. We may also collect information if you complete a survey or provide content or commentary through the provision of feedback, reviews, or customer service requests, or otherwise communicate with us.

In providing the Client Solutions, we collect information and content input to the Solution by Clients or their users as well as information generated by K12 *Insight* relating to the Client’s use of the Solution (all of which we call “**Data**”). Depending on how the Client chooses to use (or, in case of Consulting Services, direct K12 *Insight* staff to use) the Client Solutions, Data may include personal information relating to our Client’s employees, visitors, users and others. For example, when used by a School Client, Data could include first and last name, student ID number, grade level, ethnicity, address, phone number, and

email, or any combination of the same, and Let's Talk! dialogue information, which contains questions, comments, concerns, suggestions, compliments, and similar communications by any stakeholder in a school system.

We automatically collect certain types of device and usage information when you visit or use our Sites or Solutions deployed on Client websites through tracking technologies such as cookies, web beacons, pixels, and similar technologies. We collect information about your device and its software (such as your IP address, device type/model/manufacture, and unique identifier), information about the way you access and use the Service (such as visited pages, surveys, landing pages of our Clients and interest areas, referring URLs), information about your location (depending on your device settings, this could include GPS or other location data, or we may infer your location through other data such as an IP address), and analytics information. We may use third party partners to collect this information. For example, we use Google Analytics to help us measure traffic and usage trends for the Service and to understand more about the demographics of our users. You can learn more about Google's practices at <http://www.google.com/policies/privacy/partners> and view its opt-out options at <https://tools.google.com/dlpage/gaoptout>. Unfortunately, we are unable to respond to Do Not Track signals set by your browser at this time. We and our third-party partners may also use cookies and tracking technologies for advertising purposes. For more information about tracking technologies, please see Section 7 "third-party tracking and online advertising" below.

3. HOW WE USE INFORMATION

We use the information we collect, including personal information, to operate, maintain, and provide the features and functionality of the Service, to process billing and payments, to improve, market and promote our solutions and services, to inform our marketing and advertising activities; to detect and protect against fraud or misuse, and for other similar purposes. We also use information to communicate directly with you, such as to send you email messages and push notifications and permit you to communicate with others. We may send you Service-related emails or messages (e.g., account verification, change or updates to features of the Service, technical and security notices).

We use information collected through tracking technologies to remember information so that a user will not have to re-enter it during subsequent visits; provide custom, personalized content and information; to provide and monitor the effectiveness of our Service; monitor aggregate metrics such as total number of visitors, traffic, and usage on our website and our Service; diagnose or fix technology problems; help users efficiently access information after signing in, and otherwise to plan for and enhance our Service.

4. HOW WE USE CLIENT DATA

K12 *Insight* collects and processes Data solely on behalf of our Clients, and in accordance with our agreements with our Clients, in order to provide our Solutions and Service. All Data is owned and controlled by the Client and we regard Data as highly confidential. We do not use or disclose Data except as authorized and required by our Clients and as provided for in our agreements with our Clients.

We maintain a database of our Clients' information that is used only for internal business functions, such as technical support, marketing activities, billing, and to notify Clients of changes or enhancements to the services. We may use Data to improve the performance of our website and services by analyzing user behavior, including frequency of use, troubleshooting technical problems, resolving disputes and to address complaints, and to verify compliance with our Terms of Service. We may also anonymize and aggregate the Data and use such anonymized and aggregated data for our own business purposes and benchmarks.

K12 *Insight*, its staff, and authorized consultants, all of whom follow this Privacy Policy and are bound to protect Client Data in the manner indicated here, may access Data solely to provide customer support or Services requested by Client. Other than to provide technical support upon request or to process Data as part of a Consulting Service, K12 *Insight* employees and consultants do not actively access and view Data.

5. INFORMATION SHARING AND DISCLOSURE

We may share information that we collect with:

- Agents, vendors, or contractors that K12 *Insight* uses to support the operations of our business and that perform services on our behalf, which may include serving targeted advertisements, sending emails, processing payments, providing web hosting and analytic services, subject to reasonable confidentiality terms.
- Third parties as required by law or subpoena or if we reasonably believe that such action is necessary to (a) comply with the law and the reasonable requests of law enforcement; (b) to enforce our Terms of Use or other agreements or to protect the security or integrity of the K12 *Insight* Service, including to prevent harm or financial loss, or in connection with preventing fraud or illegal activity; and/or (c) to exercise or protect the rights, property, or personal safety of K12 *Insight*, our Clients, users or others.
- With other companies and brands owned or controlled by K12 *Insight*, or under common ownership and control as K12 *Insight*. These companies will use your personal information in the same way as we can under this Privacy Policy.
- Other parties in connection with a company transaction, such as a merger, sale of company assets or shares, reorganization, financing, change of control or acquisition of all or a portion of our business by another company or third party, or in the event of a bankruptcy or related or similar proceedings. If we sell, divest or transfer our business, we will require the new owner to continue to honor the terms provided in this Privacy Policy or we will provide the Client with notice and an opportunity to opt-out of the transfer of Data before the transfer occurs.

In addition, Data collected from or on behalf of a Client is shared with that Client and its authorized users. Depending on the Client's use and settings, some Data input to the Solutions may be publicly available to other Client users or to the public. We also share Data with third parties as instructed by, or at the direction of, the Client or its users. Our Client's use of such Data collected through the Service is governed by the Client's own privacy policies.

We may also share information or Data with others in an aggregated or otherwise anonymized form that does not reasonably identify you directly as an individual. For example, we may use and share aggregate or anonymized data to study and improve our Service, user functionality and product offerings.

We may share information or Data to the extent necessary to investigate, prevent or take action regarding illegal activities, suspected fraud, situations involving potential threats to the physical safety of any person, violations of our [Terms of Service](#), or as otherwise required by law. However, electronic communications made through the Let's Talk!™ Service may be deemed an "electronic communication" by K12 *Insight*. As such, K12 *Insight* reserves the right to protect Information that it believes is protected from compelled disclosure pursuant to the Electronic Communications Privacy Act, 18 U.S.C. § 2510, et seq., ("ECPA") and the Stored Communications Act, 18 U.S.C. § 2701, et seq., ("SCA"), in addition to

protections afforded by state law. The protections provided under the SCA and ECPA enable K12 *Insight* to prevent governmental authorities from seeking compelled disclosure of certain electronic communications.

6. YOUR DATA RIGHTS AND CHOICES

Modifying your information. Clients' information may be viewed and modified in our active database in real-time, at any time. The changed information may remain in archives and records for some period of time. Once survey responses have been submitted, the survey participant will not be able to access his or her participant information. If you use the Service offered by a K12 *Insight* Client, please contact the Client to request modification to your information.

Remaining anonymous. K12 *Insight* has built software features that may allow for anonymity, though these features may depend on the Client's configuration of the Service. For example, the Client may elect to either hide or make available to survey participants certain client contact information in connection with a survey. Similarly, users may be able to send communications through the Service without sharing personal information with the recipient. Please note, the identity of a user may be revealed upon reasonable belief that identification is reasonably necessary to protect the life, health or safety of K12 *Insight*, our users, or any other individual, or as may be required by law or in response to a legal request.

Control email communications. You can opt-out of receiving promotional emails from K12 *Insight* by clicking the "unsubscribe" feature at the bottom of each email. Unfortunately, you cannot unsubscribe from Service-related messaging.

Communications sent by Clients. Clients may send email or SMS/text messages to recipients through the Client Solutions and K12 *Insight* does not control those communications. Our Clients are solely responsible for all communications sent through the Service and for compliance with all applicable laws relating to such communications. To opt-out of receiving communications from a Client through the Solutions, please contact the Client directly.

7. THIRD-PARTY TRACKING AND ONLINE ADVERTISING

K12 *Insight* does not display any targeted ads on the Client Solutions.

Please note that although we may permit third party advertising partners to collect information from visitors to our website for the purpose of displaying advertisements on other websites or online services on our behalf, we take many steps to prevent such collection from users of our Client Solutions. We may display non-targeted advertisements to users on our website, while using our Services or on other sites or services.

When you visit our website, we work with third-party online advertising networks which use technology to recognize your browser or device and to collect information about your visit to our Service to provide customized content, advertising and commercial messages to you on other websites or services, or on other devices you may use. We (through the third-party advertising networks) use this information to direct our online advertisements to those people who may find them relevant to their interests.

Typically, though not always, the information is collected through cookies or similar tracking technologies. You may be able to set your browser to reject cookies or other tracking technology by actively managing the settings on your browser or mobile device. To learn more about cookies, clear

gifs/web beacons and online advertising technologies and how you may opt-out of some of this advertising, you may wish to visit the Digital Advertising Alliance's resources at www.aboutads.info/choices and/or the Network Advertising Initiative's online resources, at www.networkadvertising.org.

8. INFORMATION RETENTION AND DELETION

We will retain personal information for as long as needed to provide the Service and for our internal business purposes, which may extend beyond the termination of your subscription or user account. For example, we may retain certain data as necessary to prevent fraud or future abuse, for recordkeeping or other legitimate business purposes, or if required by law. We may also retain and use information which has been de-identified or aggregated such that it can no longer reasonably identify a particular individual. All retained personal information will remain subject to the terms of this Privacy Policy. To request deletion of your information, please email us at privacy@k12insight.com.

Data. Unless otherwise specified in writing, K12 *Insight* shall delete or de-identify Data within ninety (90) days after termination of this Agreement, in accordance with K12 *Insight's* standard data deletion and destruction practices, unless the Client provides K12 *Insight* with a written request to delete such data prior to the ninety (90) days or to follow a different deletion practice. The Client may also delete, download, or retrieve the Data at any time during the Term and for up to thirty (30) days thereafter. The Client is responsible for requesting deletion of any Data which is no longer needed for the Client's purpose.

If you use the Service offered by a K12 *Insight* Client, you may request deletion of your information by contacting the Client directly. We will cooperate with the Client to respond to this request.

We may not be able to immediately or completely delete all data in all instances, such as information retained in technical support records, customer service records, backups, and other similar business records. Similarly, we may not be able to permit information that was previously shared with others through the Services, such as the content of messages and other communications. We will not be required to delete any information which has been de-identified or disassociated with personal identifiers such that the remaining information cannot reasonably be used to identify a particular individual.

9. HOW WE STORE AND PROTECT INFORMATION

Storage and processing: Your information collected through our Service may be stored and processed in the United States or any other country in which K12 *Insight* or our affiliates or service providers maintain facilities. If you are located in the European Union or other regions with laws governing data collection and use that may differ from U.S. law, please note that we may transfer information, including personal information, to a country and jurisdiction that does not have the same data protection laws as your jurisdiction.

Keeping information safe: We care about the security of your information and employ physical, administrative, and technological safeguards designed to preserve the integrity and security of all information collected and maintained by our Service. Unique usernames and passwords must be entered each time a person logs on. Our websites are hosted in a secure server environment that uses a firewall and other technology to prevent access from outside intruders, in line with prevailing industry

standards. Internally, we use security-logs, train our employees, and limit access to K12 *Insight* personnel who need to know in order to perform their job functions. Other security safeguards include, but are not limited to, data encryption and physical and technological access controls. All of our technology and processes are not, however, guarantees of absolute security. In the event that any information under our control is compromised as a result of a breach of security, we will take reasonable steps to investigate the situation and, where appropriate, notify our Client or individual users whose information may have been compromised and take other steps, in accordance with any applicable laws and regulations and our agreements with our Clients. Clients must actively protect their information by maintaining the confidentiality of all usernames and passwords and by adequately installing the appropriate anti-virus programs and security measures on their own systems. You must immediately notify K12 *Insight* if any information security breach is suspected.

10. HOW WE PROTECT STUDENT DATA AND COMPLY WITH LAWS

When the Service is used by Clients that are providers of educational services, such as schools, school districts, or teachers (collectively referred to as “**School Clients**”), we may collect or have access to Data that includes personal information of students, which may be provided by the School Client or by a student, parent, guardian or other user (“**Student Data**”). While we consider all Client Data to be confidential and in general do not use such data for any purpose other than improving and providing our Services to our Clients, we exercise special caution to protect Student Data.

Student Data privacy principles. We are committed to the following principles to protect Student Data:

- We collect, maintain, use, and share Student Data only to provide and support the Service as described in our Privacy Policy, to maintain, develop, support or improve our websites, services and applications, and as otherwise permitted by our agreements or with the consent of the parent, guardian, student or School Client.
- We do not use or disclose Student Data for targeted advertising purposes. While we do permit third-party advertising partners to operate on our website for the purpose of retargeting, analytics, and attribution services, we do not engage third party advertising partners to collect information through our Solution Services.
- We do not build a personal profile of a student other than in furtherance of the School Client’s use of the Service, or as authorized by a student or parent.
- We maintain a comprehensive data security program designed to protect the types of Student Data maintained by the Service.
- We will clearly and transparently disclose our data policies and practices to our users.
- We will never sell Student Data unless the sale is part of a corporate transaction, such as a merger, acquisition, bankruptcy, or other sale of assets, in which case we will require the new owner to continue to honor the terms provided in this Privacy Policy or we will provide the School Client with notice and an opportunity to opt-out of the transfer of Student Data by deleting the Student Data before the transfer occurs.

- We will not make any material changes to our Privacy Policy or contractual agreements that relate to the collection or use of Student Data without first giving notice to the School Client and providing a choice before the Student Data are used in a materially different manner than was disclosed when the information was collected.

How we use and disclose Student Data. We use and disclose Student Data as described in our Privacy Policy under Section 4 “How We Use Client Data” and Section 5 “Information Sharing and Disclosure.”

How we retain and delete Student Data. We do not knowingly retain Student Data beyond the time period required to support the School Client’s purpose, unless authorized by a School Client, student, or parent. Unless otherwise directed by a School Client, we will delete or de-identify Student Data after the termination of our agreement with the School Client, in accordance with the terms of any applicable written agreement with the School Client, written requests from authorized School Client administrators, and our standard data retention schedule.

School Clients can request account or data deletion at any time by contacting us at privacy@k12insight.com. We may not be able to immediately or completely delete all data in all instances, such as information retained in technical support records, customer service records, backups, and other similar business records. Similarly, we may not be able to delete information that was previously shared with others through the Services, such as the content of messages and other communications. We will not be required to delete any information which has been de-identified or disassociated with personal identifiers such that the remaining information cannot reasonably be used to identify a particular individual.

Compliance with laws. We do not use Student Data for any purpose other than to provide the Services, in accordance with contractual agreements with our School Clients. K12 *Insight* does not own or control Student Data, which belongs to the individual student and/or the School Client. As specified in our agreements with School Clients, the K12 *Insight* Service is designed to provide protections for Student Data as required by various applicable privacy laws. For example:

- **The Family Educational Rights and Privacy Act (“FERPA”).** This Privacy Policy and our Service are designed to meet our responsibilities to protect personal information from the students' educational records under FERPA. We agree to work with our School Clients to jointly ensure compliance with the FERPA regulations.
- **Children’s Online Privacy Protection Act (“COPPA”).** K12 *Insight* is not directed to children under 13 and does not knowingly collect any information from children under the age of 13. To the extent a School Client uses the Service to collect personal information from children under the age of 13 or sends communications through the Service to children under the age of 13, the School Client provides the requisite consent for K12 *Insight* to collect and use such personal information from students under 13 for the purpose of providing the Service and as otherwise described in this Agreement, as permitted by COPPA.
- **Students Online Personal Information Protection Act (“SOPIA”).** This Privacy Policy and our Service are designed to comply with SOPIA. We do not use Student Data for targeted advertising purposes. We do not use collected information to amass a profile of a K-12 student except in furtherance of providing the features and functionality of the Service. We never sell Student Data unless the sale is part of a corporate transaction, such as a merger, acquisition,

bankruptcy, or other sale of assets, in which case we make efforts to ensure the successor entity honors the privacy commitments made in this policy and/or we will notify the School Client and provide an opportunity to opt-out by deleting student accounts before the data transfer occurs.

- **California Assembly Bill 1584 ("AB 1584").** This Privacy Policy and our Service are designed to comply with AB 1584. Pupil records obtained by K12 *Insight* from a local educational agency ("LEA") continue to be the property of and under the control of the LEA. Parents, legal guardians, or eligible pupils may review personally identifiable information in the pupil's records and correct erroneous information by contacting their LEA directly. In the event of an unauthorized disclosure of a pupil's records, K12 *Insight* will notify the LEA and will provide the LEA with information to be shared with the affected parent(s), legal guardians(s) or eligible pupil(s). Pupil records will be deleted and/or de-identified in accordance with our agreements with each School Client and as described in this Privacy Policy.

If you have any questions about our practices with regard to Student Data, please contact us at privacy@k12insight.com.

10. CHANGES TO OUR PRIVACY POLICY.

As we are constantly improving the Services and expanding our business, K12 *Insight* reserves the right to modify this Privacy Policy from time to time to reflect such improvements. In the event we make such changes, we will announce the changes and post the new policy at <https://www.k12Insight.com/privacy-policy>. We will also use our best efforts to provide advance notice of any material changes to this Privacy Policy, to permit you a reasonable chance to review before such changes go into effect. If you object to any changes, you may close your account and/or discontinue your use of the Service. Continuing to use our Service after we publish changes to this Privacy Policy means that you are consenting to the changes.

K12 *Insight* shall not make any material change to the Privacy Policy or our practices that involve the collection or use of Student Data without first giving thirty (30) days' notice to School Client and providing a choice before the Student Data is used in a materially different manner than was disclosed when the information was collected.

Last Updated: December 15, 2019

Effective Date: January 1, 2020