TEXAS STUDENT DATA PRIVACY AGREEMENT
Version 2.0

Frisco Independent School District

AND

Lightspeed Systems

Date: 31-Mar-2020

This Texas Student Data Privacy Agreement (“DPA”) is entered into by and between the **Frisco Independent School District** (hereinafter referred to as “LEA”) and **Lightspeed Solutions, LLC (d/b/a Lightspeed Systems)** based at address: 2500 Bee Cave Road, Building One, Suite 350, Austin TX 78746, Unites States (hereinafter referred to as “Provider”), (jointly referred to as the “Parties”) on the 31-Mar-2020. The Parties agree to terms as stated herein.

RECITALS

WHEREAS, the Provider has agreed to provide the Local Education Agency (“LEA”) with certain digital education services (“Services”) as described in Article I and Exhibit “A”; and

WHEREAS, in order to provide the Services described in the Service Agreement, the Provider may receive or create, and the LEA may provide documents or data that are covered by several federal statutes, among them, the Family Education Rights and Privacy Act (“FERPA”) at 20 U.S.C. §1232g (34 C.F.R. Part 99), Children’s Online Privacy Protection Act (“COPPA”), 15 U.S.C. §§6501-6506; Protection of Pupil Rights Amendment (“PPRA”), 20 U.S.C. §1232h; and

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

WHEREAS, for the purposes of this DPA, the Provider is a school official with legitimate educational interests in accessing educational records pursuant to the Service Agreement; and

WHEREAS, the Parties wish to enter into this DPA to ensure that the Service Agreement conforms to the requirements of the privacy laws referred to above and to establish implementing procedures and duties; and

WHEREAS, the Provider may, by signing the “General Offer of Privacy Terms” (Exhibit “E”), agree to allow other LEAs in Texas the opportunity to accept and enjoy the benefits of this DPA for the Services described herein, 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. **Purpose of DPA.** The purpose of this DPA is to describe the duties and responsibilities to protect Student Data transmitted to Provider from LEA pursuant to the Service Agreement, including compliance with all applicable statutes, including the FERPA, PPRA, COPPA and other applicable Texas State laws, all as may be amended from time to time. In performing these services, the Provider shall be considered a School Official with a legitimate educational interest performing services otherwise undertaken by the LEA. With respect to the use and maintenance of Student Data, the Provider shall be under the direct control and supervision of the LEA.

2. **Nature of Services Provided.** The Provider has agreed to provide the following digital educational products and services described below and as may be further outlined in Exhibit “A” hereto:

3. **Student Data to be Provided.** The Parties shall indicate the categories of Student Data to be provided in the Schedule of Data, attached hereto as Exhibit "B".

4. **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 term used in the Service Agreement.

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 Agreement 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 pursuant to 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. Provider may transfer pupil-generated content to a separate account, according to the procedures set forth below.

2. **Parent Access.** LEA shall establish reasonable procedures pursuant to which a parent, legal guardian, or eligible student may review and/or copy Student Data in 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. Provider shall respond in a timely manner (and no later than 28 business days from the date of the request) to the LEA's request for Student Data in a pupil's records held by the Provider to review or correct as necessary. In the event that a parent of a pupil or other individual contacts the Provider to review and/or copy any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, which will follow the necessary and proper procedures regarding the requested information.

3. **Separate Account.** In the event pupil generated content is stored or maintained by the Provider as part of the Services described in Exhibit "A," and to the extent the capability to provide a separate account is available, Provider shall, in response to a verified request of the LEA, transfer said pupil generated content to a separate student account upon termination of the Service Agreement; provided that, such transfer shall only apply to pupil generated content that is severable from the Service.

4. **Third Party Request.** Should a Third Party, including law enforcement and government entities, contact the Provider with a request (including subpoena) for data held by the Provider pursuant to the Services, the Provider shall redirect the Third Party to seek the data directly from the LEA. Provider shall notify the LEA in advance of a compelled disclosure to a Third Party, unless legally prohibited and shall provide the LEA with a copy of the court order requiring such disclosure. 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.

5. **Sub-processors.** The LEA agrees that from time to time, it may be necessary for the Provider to utilize Sup-processors. Before a Sub-processor performs any functions involving Student Data, the Provider shall reasonably vet the privacy and security practices of the Sub-processor to ensure those practices protect Student Data consistent with Provider obligations. Sub-processors shall not be considered Third Parties.

6. **Provider Materials**. Provider retains all right, title and interest in and to any and all of Provider's software, materials, tools, forms, documentation, training and implementation materials and intellectual property ("Provider Materials"). Provider grants to the LEA a personal, nonexclusive license to use the Provider Materials for its own non-commercial, incidental use as set forth in the Service Agreement. Provider 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.

7. **Data Portability**. Provider shall, at the request of the LEA, make Data available including Pupil Generated Content in a readily accessible format; provided, however, that such transfer shall only apply to content that is severable from the service.

8. **No Unauthorized Use**. Provider shall not use LEA data or information for any purpose other than as explicitly specified in this DPA.

ARTICLE III: DUTIES OF LEA

1. **Privacy Compliance.** 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 applicable Texas privacy statutes.

2. **Annual Notification of Rights.** If the LEA has a policy of disclosing education records under FERPA (34 C.F.R. § 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 obtaining access to the services and hosted data.

4. **Unauthorized Access Notification.** LEA shall notify Provider promptly of any known or suspected 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 state and federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRA, Texas Education Code Chapter 32, and all other applicable Texas privacy statutes.

2. **Authorized Use.** The data made available pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services stated in this DPA and/or otherwise authorized under the statutes and applicable implementing regulations referred to above in subsection 1. Provider also acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, meta data, user content or other non-public information and/or personally identifiable information contained in the Student data, without the express written consent of the LEA, unless it fits into the de-identified information exception in Article IV Section 4, there is a court order or lawfully issued subpoena for the information.

3. **Employee Obligation.** Provider shall require all employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the data shared under this DPA. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the DPA.

4. **No Disclosure.** De-identified information may be used by the Provider for the purposes of development, research, and improvement of educational sites, services, or applications, as any other member of the public or party would be able to use de-identified data pursuant to 34 C.F.R. § 99.31(b). Provider shall not attempt to re-identify de-identified Student Data and shall not 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 LEA which has provided prior written consent for such transfer. Provider shall not copy, reproduce or transmit any data obtained under the Service Agreement and/or any portion thereof, except as necessary to fulfill the Service Agreement.

5. **Disposition of Data.** Provider shall, following LEA's written, verified request and in accordance with the applicable terms below in subsections a. or b., Provider shall dispose or delete all Student Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained, unless Provider is required to retain such information for legal or regulatory reasons, or to enforce this DPA, or the LEA has asked the Provider to retain the Student data. The method of disposition shall include: (1) the shredding of any photocopies of any Student Data; (2) Erasing; or (3) Otherwise modifying the personal information in those records to make it unreadable or indecipherable by human or electronic/digital means. Nothing in the Agreement authorizes Provider to maintain Student Data obtained under the Agreement beyond the time period reasonably needed to complete the disposition. Provider shall provide written notification (email is acceptable) to LEA when the Student Data has been disposed. The duty to dispose of Student 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 Student Data" form, a copy of which is attached hereto as Exhibit "D." Within fourteen (14) calendar days after the date of a request from the LEA, the Provider shall provide the LEA with any specified portion of the Student Data.

   a. **Partial Disposal During Term of Service Agreement.** Throughout the Term of the Service Agreement, LEA may require partial disposal of Student Data that is no longer needed which was obtained pursuant to the Service Agreement. Partial disposal of data shall be subject to LEA's request to transfer data to a separate account, pursuant to Article II, section 3.

b. **Complete disposal Upon Termination of Service Agreement.** Upon Termination of the Service Agreement, Provider shall dispose of or delete all Student Data obtained under the Service Agreement. Prior to disposition of the data, Provider shall notify LEA in writing (email is acceptable) of its option to transfer data to a separate account, pursuant to Article II, section 3

c. **If no written request is received**, Provider shall dispose of or delete all Personally Identifiable Information within Student Data obtained under the Agreement at the earliest of (a) in accordance with its applicable data deletion policy, which requires deletion no later than when it is no longer needed for the purpose for which it was obtained or (b) as required by applicable law.

6. **Advertising Prohibition.** Provider is prohibited from using or selling Student Data to: (a) market or advertise to students or their families/guardians; (b) inform, influence, or enable marketing, advertising, or other commercial efforts by a Provider; (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 Student Data for the development of commercial products or services, other than as necessary to provide the Service to LEA. This section does not prohibit Provider from using Student Data for adaptive learning or customized student learning purposes.

ARTICLE V: DATA PROVISIONS

1. **Data Security.** The Provider shall abide by and maintain adequate data security measures, consistent with industry standards and technology best practices, to protect Student Data from unauthorized disclosure or acquisition by unauthorized persons or entities. The general security duties of Provider are set forth below. Provider may further detail its security programs and measures in Exhibit “F” hereto. The applicable measures shall include, but are not limited to the following:

a. **Passwords and Employee Access.** Provider shall use commercially reasonable precautions to secure usernames, passwords and any other means of gaining access to the Services or to Student Data as outlined in the Provider’s Security Policy. Provider shall only provide access to Student Data to employees, contractors or Sub-processors that are performing the services underlying the Services. Employees with access to Student Data shall have signed confidentiality agreements. Provider shall conduct criminal background checks of employees prior to providing access to Student Data and prohibit access to Student Data by any person with criminal or other relevant unsatisfactory information that presents an unreasonable risk to LEA or its Users.

b. **Destruction of Data.** Provider shall destroy or delete all Student Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained or transfer said data to LEA or LEA’s designee, according to the procedure identified in Article IV, section 5. Nothing in the Service Agreement authorizes Provider to maintain Student Data beyond the time period reasonably needed to complete the disposition.

c. **Security Protocols.** The parties shall maintain security protocols that meet industry standards regarding the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. Provider shall maintain all data obtained or generated pursuant to the Service Agreement in a secure digital environment and not copy, reproduce, or transmit data obtained pursuant to the Service Agreement, except as necessary to fulfill the purpose of data requests by LEA.

d. **Employee Training.** The Provider shall provide recurring, periodic (no less than annual, with additional sessions as needed throughout the year to address relevant issues/changes, such as (but not necessarily limited to) new or evolving security threats, changes to security protocols or practices, changes to software and/or hardware, identified vulnerabilities, etc.) security training to those of its employees who operate or have access to the system. Such trainings must be tailored to the Provider's business and cover, but not necessarily be limited to, the following topics: common types of attackers (e.g., cyber criminals, hacktivists, government sponsored groups, inside threats, etc.); common types of attacks (e.g., social engineering, spoofing, phishing, etc.) and how the information sought is typically used; identifying threats, avoiding threats, physical security and environmental controls; internal policies and procedures; and safe internet habits. Further, Provider shall provide LEA with contact information of an employee who LEA may contact if there are any security concerns or questions.

e. **Security Technology.** When the service is accessed using a supported web browser, Provider shall employ industry standard measures to protect data from unauthorized access. The service security measures shall include server authentication and data encryption. Provider shall host data pursuant to the Service Agreement in an environment using a firewall that is updated according to industry standards.

f. **Security Coordinator.** If different from the designated representative identified in Article VII, section 6(a), Provider shall provide the name and contact information of Provider's Security Coordinator for the Student Data received pursuant to the Service Agreement.

g. **Sub-processors Bound.** Provider shall periodically conduct or review compliance monitoring and assessments of Sub-processors to determine their compliance with this Article in accordance with Provider's vendor review policy.

h. **Periodic Risk Assessment.** Provider shall conduct risk assessments and remediate identified security and privacy vulnerabilities in accordance with the Provider's Vulnerability Remediation Policy.

i. **Audits.** Upon receipt of a request from the LEA, and at the expense of the LEA, 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. The Provider 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 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 Provider.

LEA shall enter into a non-disclosure agreement with Provider prior to the commencement of any such audit.

j. **Backups.** Provider agrees to maintain backup copies, in accordance with Provider's data deletion policy, of LEA's data in case of a failure of Provider's system or any other unforeseen event resulting in loss of Student Data or any portion thereof.

2. **Data Breach.** In the event that Student Data is accessed or obtained by an unauthorized individual, Provider shall provide notification to LEA within a reasonable amount of time of the incident, as required by the applicable state or federal laws. Provider shall follow its written Incident Response Plan in reporting the incident.

   a. Provider agrees to adhere to state and federal law with respect to data breach related to the Student Data, including, notification timeframe when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
   b. Upon signing a non-disclosure agreement, LEA may be provided a copy of the written Incident Response Plan.

ARTICLE VI – GENERAL OFFER OF PRIVACY 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 this DPA to any other LEA who signs the acceptance on said Exhibit, in accordance with Article VII, Section 6(b) Notification of Acceptance of General Offer of Terms. The Form is limited by the terms and conditions described therein.

ARTICLE VII: MISCELLANEOUS

1. **Term.** The Provider shall be bound by this DPA for the duration of the Service Agreement or so long as the Provider maintains any Student Data.

2. **Termination.** In the event that either party seeks to terminate this DPA, they may do so by mutual written consent and as long as any Terms of Use or other agreement, to the extent one exists, has lapsed or has been terminated. Either Party (the "Non-breaching Party") may terminate this DPA and the Terms of Use or other agreement, to the extent one exists, effective immediately upon delivery of written notice to the other Party ("Breaching Party") if the Breaching Party materially breaches any provision of the Agreement and does not cure the breach within thirty (30) days after receiving written notice thereof from the Non-Breaching Party.

3. **Effect of Termination Survival.** If the Service Agreement is terminated, the Provider shall destroy all of LEA's data pursuant to Article II, section 3, and Article V, section 1b.

4. **Priority of Agreements.** This DPA shall govern the treatment of student data in order to comply with privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the DPA and the Service Agreement, the DPA shall apply and take precedence. Except as described in this section 4, all other provisions of the Service Agreement shall remain in effect.

5. **Limited Authority to Renegotiate.** Notwithstanding any other provision of this Agreement, if any federal, state, or local government or agency passes, issues, or promulgates any law, rule, regulation, standard of interpretation, or materially changes its current position as to the interpretation of any existing law, rule, regulation or standard, including but not limited to FERPA, PPRA and COPPA at any time while this Agreement is in effect in a manner that would prohibit, restrict, limit or render illegal the relationship described herein, or if any governmental entity issues a written allegation or otherwise provides notice to the parties to the effect that the relationship described herein is in violation of any law, rule or regulation, then either party may give the other party notice of intent to amend this Agreement to bring it into compliance with all applicable laws. If this Agreement is not amended in writing by mutual agreement within thirty (30) days after notice is given, then the party giving notice shall have the right to terminate the Agreement effective at the end of the thirty (30) day renegotiation period.

6. **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 below.

   a. **Designated Representatives**

The designated representative for the **LEA** for this Agreement is:

Name: **Naomi Harper**
Title: Director of Legal Affairs & Senior Counsel
Contact Information:
5515 Ohio Drive Frisco,
TX 75305
Email: harpern@friscoisd.org
Phone Number: 469.633.6052

The designated representative for the **Provider** for this Agreement is:

Name: **John Genter**
Title: VP Global Operations
Contact Information:
2500 Bee Cave Road, Building 1, Suite 350
Austin, TX 78746, United States
Email:privacy@lightspeedsystems.com | Jgenter@lightspeedsystems.com
Phone Number: 737.205.2500

   b. **Notification of Acceptance of General Offer of Terms.** Upon execution of Exhibit E, General Offer of Terms, Subscribing LEA shall provide notice of such acceptance in writing and by personal delivery, or e-mail transmission (if contact information is provided for the specific mode of delivery), or first-class mail, postage prepaid, to the designated representative below. Any notice delivered hereunder shall be deemed effective, as applicable, upon delivery, if personally delivered; upon receipt as evidenced by the date of transmission indicated on the transmission material, if by e-mail; or four (4) days after mailing, if by first-class mail, postage prepaid.

The designated representative for the notice of acceptance of the General Offer of Privacy Terms is:

Name: **John Genter**
Title: VP Global Operations
Contact Information:
2500 Bee Cave Road, Building 1, Suite 350
Austin, TX 78746, United States
Email:privacy@lightspeedsystems.com | Jgenter@lightspeedsystems.com
Phone Number: 737.205.2500

7. **Entire Agreement.** This DPA 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 at any time.

8. **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 interpreted 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 interpreted without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.

9. **Governing Law: Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS 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 THE LEA IS LOCATED FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS SERVICE AGREEMENT OR THE TRANSACTIONS CONTEMPLATED HEREBY.

10. **Authority.** Provider represents that it is authorized to be bound to the terms of this Agreement, including confidentiality and destruction of Student Data and any portion thereof contained herein, all related or associated institutions, individuals, employees, contractors, subcontractors or sub-processors who may have access to the Student Data and/or any portion thereof, or may own, lease or control equipment or facilities of any kind where the Student Data and/or portion thereof stored, maintained, or used in any manner whatsoever. Provider agrees that any purchaser of the Provider shall also be bound to the Agreement.

11. **Waiver.** No delay or omission of the LEA to exercise any right hereunder shall be construed as a waiver of any such right and the LEA reserves the right to exercise any such right from time to time, as often as may be deemed expedient.

12. **Successors Bound.** This DPA is and shall be binding upon the respective assigns or 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 Provider.

13. **Electronic Signature**: The parties understand and agree that they have the right to execute this Agreement through paper or through electronic signature technology, which is in compliance with State and Federal law governing electronic signatures. The parties agree that to the extent they sign electronically, their electronic signature is the legally binding equivalent to their handwritten signature. Whenever they execute an electronic signature, it has the same validity and meaning as their handwritten signature. They will not, at any time in the future, repudiate the meaning of my electronic signature or claim that their electronic signature is not legally binding. They agree not to object to the admissibility of this Agreement as an electronic record, or a paper copy of an electronic document, or a paper copy of a document bearing an electronic signature, on the grounds that it is an electronic record or electronic signature or that it is not in its original form or is not an original.

    Each party will immediately request that their electronic signature be revoked in writing if they discover or suspect that it has been or is in danger of being lost, disclosed, compromised or subjected to unauthorized use in any way. They understand that they may also request revocation at any time of their electronic signature for any other reason in writing.

    If either party would like a paper copy of this Agreement, they may request a copy from the other party.

14. **Multiple Counterparts**: This Agreement may be executed in any number of identical counterparts. If so executed, each of such counterparts shall constitute this Agreement. In proving this Agreement, it shall not be necessary to produce or account for more than one such counterpart. Execution and delivery of this Agreement by .pdf or other electronic format shall constitute valid execution and delivery and shall be effective for all purposes (it being agreed that PDF email shall have the same force and effect as an original signature for all purposes).

[Signature Page Follows]

IN WITNESS WHEREOF, the parties have executed this Texas Student Data Privacy Agreement as of the last day noted below.

Lightspeed Solutions, LLC (d/b/a Lightspeed Systems):

BY: ____________________________ Date: 31-Mar-2020

Printed Name: **Gregory Funk** Title/Position**: VP, Global Finance**

Frisco Independent School District

BY: Naomi Harper Date: 31-Mar-2020

Printed Name: **Naomi Harper** Title/Position: **Director of Legal Affairs & Senior Counsel**

EXHIBIT “A”

DESCRIPTION OF SERVICES

Lightspeed Systems, integrated solutions for K-12 school networks:

• Analytics	www.lightspeedsystems.com/analytics/
• Mobile Manager	www.lightspeedsystems.com/manage/
• Relay Filter	www.lightspeedsystems.com/filter/
• Relay Classroom	www.lightspeedsystems.com/monitor/
• Relay Safety Check	www.lightspeedsystems.com/protect/
• Web Filter	www.lightspeedsystems.com/filter/

EXHIBIT "B"

SCHEDULE OF DATA

Category of Data	**Elements**	**Check if used by your system**
Application Technology Meta Data	IP Addresses of users. Use of cookies, etc.	**X**
	Other application technology meta data- Please specify:	**X**
Application Use Statistics	Meta data on user interaction with application	**X**
Assessment	Standardized test scores	
	Observation data	
	Other assessment data- Please specify:	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications that are captured (emails, blog entries)	**X**
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	Place of Birth	
	Gender Ethnicity or race	
	Language information (native, preferred or primary language spoken by student)	
	Other demographic information- Please specify:	
Enrollment	Student school enrollment	**X**
	Student grade level	
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information- Please specify:	

Category of Data	Elements	Check if used by your system
Parent/Guardian Contact Information	Address	
	Email	
	Phone number	
	State ID Number	
	Provider/App assigned student ID number	
	Student app username	
	Student app passwords	
Parent/Guardian ID	Parent ID number (created to link parents to students)	
Parent/Guardian Name	First and/or Last	
Schedule	Student scheduled courses	
	Teacher names	
Special Indicator	English language learner information	
	Low income status	
	Medical alerts/health data	
	Student disability information	

Category of Data	Elements	Check if used by your system
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information – Please specify:	
Student Contact Information	Address	
	Email	X
	Phone	
Student Identifiers	Local (School district) ID Work data- Please specify:	X
Student Name	First and/or Last	X
Student In App Performance	Program/application performance (typing program- student types 60 wpm, reading program- student reads below grade level)	
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	

Category of Data	**Elements**	**Check if used by your system**
Student work	Student generated content; writing, pictures, etc.	
	Other student work data: Please specify	
Transcript	Student course grades Student course data Student course grades/performance scores Other transcript data – Please specify:	
Transportation	Student pick up and/or drop off location	
	Student bus card ID number Other transportation data – Please specify:	
Other	Please list each additional data element used, stored or collected by your application. If additional space is needed, use space below.	**X**

No Student Data Collected at this time________________.
*Provider shall immediately notify LEA if this designation is no longer applicable. OTHER:

Use space below, if more space is needed:

List of Student Information Fields

a) Unique SIS User ID
b) Username
c) First Name
d) Last Name
e) School
f) School or District Office Billing Zip Code
g) Grade Level, Class, or Group (optional)
h) E-mail Address (optional)
i) User Type (student or staff)
j) Authentication (Directory Service authentication / Local authentication) (Recommended)
k) Websites that users at the school visited
l) Websites that each user visited and time spent on page
m) Specific Search Queries of Users
n) Information about the web traffic on the network (by user, by category, etc.)
o) Device Location Data

Web Filtering Products
Rocket

- With SIS integration – A-N
- Without SIS integration – E / F / I / K
- The hardware appliance is on premise and managed by the customer and they have full access to this data and manage any sharing of this data including access by Lightspeed Systems employees and that access is limited to support needs.

SaaS Products

- We use a shared user information database across our SaaS products and features. This includes Mobile Manager, Relay, Launch, Analytics and Classroom. Customers will commonly sync student records to this shared database for classroom specific management capabilities across these products. Customers have full access to and manage this data. Lightspeed Systems employee access to this data is limited to support needs.
- We do not share this information with any 3rd party unless specifically directed by the customer and requiring a signed document from the customer to initiate the sharing. The personal contact information collected by this can include Network Username or Email Address, First and Last Name, School Grade or Year Level, Class or Group Memberships.

Relay

- Filter – B (H mandatory) / C / D / I (user or Admin) / K / L / M / GAFE OU / Time on App
- Google Classroom – B (H mandatory) / C / D / I / Class Name
- O – if enabled
- Flagged Browsing content either posted or reviewed on websites

MDM

- With SIS integration – A-J and O
- Without SIS integration – only F
- Additional Information from devices using MDM
- Apps distributed to user (Managed by User) or to a particular device (Managed by Device)
- Type of Device
- Version of Operating System

Classroom

- With SIS integration – A-J
- Without SIS integration – only F and either H or B
- In addition to the shared SaaS information collected above Classroom Orchestrator may collect screenshots of computer usage that could contain personal information.
- Access to this information is limited to the organization and group admins defined by the customer and when necessary for support reasons can be shared with a Lightspeed Systems employee.

EXHIBIT "C"

DEFINITIONS

Commercial Purpose: Using information for a commercial purpose means to advance a person's commercial or economic interests, such as by inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction.

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 Provider 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 Provider'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.

Educational Records: Educational Records are official records, files and data directly related to a student and maintained by the 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. For purposes of this DPA, Educational Records are referred to as Student Data.

HB 2087: The statutory designation for what is now Texas Education Code Chapter 32 Data relating to student information.

NIST: Draft National Institute of Standards and Technology ("NIST") Special Publication Digital Authentication Guideline.

Operator: The term "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 primarily for K-12 school purposes and was designed and marketed for K-12 school purposes. For the purpose of the Service Agreement, the term "Operator" is replaced by the term "Provider." This term shall encompass the term "Third Party," as it is found in applicable State statutes.

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 Provider's software, website, service, or app, including mobile apps, whether gathered by Provider 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.

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

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.

Pupil Records: Means both of the following: (1) Any information that directly relates to a pupil that is maintained by LEA and (2) any information acquired directly from the pupil through the use of instructional software or applications assigned to the pupil by a teacher or other LEA employee. For the purposes of this Agreement, Pupil Records shall be the same as Educational Records, Student Personal Information and Covered Information, all of which are deemed Student Data for the purposes of this Agreement.

School Official: For the purposes of this Agreement and pursuant to 34 C.F.R. § 99.31(a)(1)(B), a School Official includes 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 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.

SDPC (The Student Data Privacy Consortium): Refers to the national collaborative of schools, districts, regional, territories and state agencies, policy makers, trade organizations and marketplace Providers addressing real-world, adaptable, and implementable solutions to growing data privacy concerns.

Service Agreement: Refers to the Contract or Purchase Order to which this DPA supplements and modifies.

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

Sub-processor: For the purposes of this Agreement, the term "Sub-processor" (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 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 Provider'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 2 CTO Council is the organization that sponsors TXSPA and the TXSPA is the Texas affiliate of the National Student Privacy Consortium.

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 pupil records. However, for the purpose of this Agreement, 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

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

Extent of Disposition Disposition shall be:	____ Partial. The categories of data to be disposed of are as follows: ____ Complete. Disposition extends to all categories of data.
Nature of Disposition Disposition shall be by:	____ Destruction of deletion of data. ____ Transfer of data. The data shall be transferred as set forth in an attachment to this Directive. Following confirmation from the LEA that data has been successfully transferred, Provider shall destroy or delete all applicable data.
Timing of Disposition Data shall be disposed of by the following date:	____ As soon as commercially practicable ____ By (Insert Date)____________

_________________________________ _________________
Authorized Representative of LEA Date

_________________________________ _________________
Verification of Disposition of Data Date
by Authorized Representative of Provider

EXHIBIT “E”

GENERAL OFFER OF PRIVACY TERMS

1. **Offer of Terms**

Lightspeed Solutions, LLC (d/b/a Lightspeed Systems) offers the same privacy protections found in this DPA between it and Frisco Independent School District, to any other LEA (“Subscribing LEA”) which accepts this 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 other LEA may also agree to change the data provided by LEA to the Provider in Exhibit “B” to suit the unique needs of the LEA. The Provider may withdraw the General Offer in the event of any of the following: (1) a material change in the applicable privacy statutes; (2) a material change in the services and products subject listed in the Originating Service Agreement; or three (3) years after the date of Provider’s signature to this Form. Provider shall notify ________________ in the event of any withdrawal so that this information may be transmitted to the appropriate users.

Provider: **Lightspeed Solutions, LLC (d/b/a/ Lightspeed Systems**)

By: ______________________ Date: 31-Mar-2020

Printed Name: **Gregory Funk** Title/Position: **VP, Global Finance**

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.

Subscribing LEA: ____

(Insert Subscribing LEA)

By: ______________________ Date: ____________________

Printed Name: __________________ Title/Position: ______________________________

TO ACCEPT THE GENERAL OFFER, THE SUBSCRIBING LEA MUST DELIVER THIS SIGNED EXHIBIT TO THE PERSON AND EMAIL ADDRESS LISTED BELOW.

Name: __________________________

Title: ___________________________

Email Address: ___________________

EXHIBIT "F"

Data Security Requirements

Having robust data security policies and controls in place are the best ways to ensure data privacy. Please answer the following questions regarding the security measures in place in your organization:

1. Does your organization have a data security policy? x **Yes** □ No

   - If yes, please provide it.
   - Upon signing and NDA the policy can be made available.

2. Has your organization adopted a cybersecurity framework to minimize the risk of a data breach? If so which one(s):

____ ISO 27001/27002
____ CIS Critical Security Controls
____ NIST Framework for Improving Critical Infrastructure Security
__x__ Other: _**We utilize both CIS and NIST** ____________

3. Does your organization store any customer data outside the United States?
□ Yes x **No**

4. Does your organization encrypt customer data both in transit and at rest? x **Yes** □ No

5. Please provide the name and contact info of your Chief Information Security Officer (CISO) or the person responsible for data security should we have follow-up questions.

   Name/Title: **John Genter, VP Global Operations**
   Contact information:
   Email: security@lightspeedsystems.com or jgenter@lightspeedsystems.com
   Phone #: 737.205.2500