VIRGINIA STUDENT DATA PRIVACY AGREEMENT
Version 1

Fauquier County Public School District

AND

Lightspeed Systems

Date: 25-Mar-2020

This Student Data Privacy Agreement ("DPA") is entered into by and between the **Fauquier County Public 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 25-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, the Individuals with Disabilities Education Act ("IDEA"), 20 U.S.C. §§ 1400 et. seq.; and

WHEREAS, the documents and data transferred from LEAs and created by the Provider's services are also subject to Virginia student privacy laws, including the 1002Code of Virginia § 22.1-289.01. *School service providers; school-affiliated entities; student personal information; and § 22.1-287.02. Students' personally identifiable information*.; 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 Virginia 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 (as defined in Exhibit "C") transmitted to Provider from the LEA pursuant to the Service Agreement, including compliance with all applicable state privacy statutes, including the FERPA, PPRA, COPPA, IDEA, 603 C.M.R. 23.00, 603 CMR 28.00, and Code of Virginia § 22.1-289.01. School service providers; school-affiliated entities; student personal information; and § 22.1-287.02. Students' personally identifiable information. In performing these services, to the extent Personally Identifiable Information (as defined in Exhibit "C") from Pupil Records (as defined in Exhibit "C") are transmitted to Provider from LEA, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall

be under the direct control and supervision of the LEA.

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. **LEA Data Property of LEA**. All Student Data, user generated content or any other Pupil Records transmitted to the Provider pursuant to this Agreement is and will continue to be the property of and under the control of the LEA, or to the party who provided such data (such as the student, in the case of user generated content.). The Provider further acknowledges and agrees that all copies of such Student Data or any other Pupil Records transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are also subject to the provisions of this Agreement in the same manner as the original Student Data or Pupil Records. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data or any other Pupil Records contemplated per this Agreement shall remain the exclusive property of the LEA. For the purposes of FERPA and state law, the Provider shall be considered a School Official, under the control and direction of the LEA as it pertains to the use of Student Data notwithstanding the above.

2. **Parent Access**. Provider shall cooperate and respond within fourteen (14) days to the LEA's request for personally identifiable information in a pupil's records held by the Provider to view or correct as necessary. In the event that a parent of a pupil or other individual contacts the Provider to review any of the Pupil Records of Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.

3. **Separate Account**. Provider shall, at the verified request of the LEA, transfer Student Generated Content to a separate student account , to the extent the capability to provide a separate account is available ,when required by the Code of Virginia § 22.1-289.01. School service providers; school-affiliated entities, 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**. Provider shall notify the LEA in advance of a compelled disclosure to a Third Party, unless legally prohibited.

5. **Subprocessors**. Provider shall enter into written agreements with all Subprocessors performing functions pursuant to this DPA, whereby the Subprocessors agree to protect

Student Data in manner consistent with the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Privacy Compliance**. LEA shall provide data for the purposes of the DPA and any related contract in compliance with the FERPA, PPRA, IDEA, Code of Virginia § 22.1-289.01. School service providers; school-affiliated entities; student personal information; and § 22.1-287.02. Students' personally identifiable information, and all other applicable Virginia statutes.

2. **Annual Notification of Rights** LEA shall ensure that its annual notice under FERPA defines vendors, such as the Provider, as "School Officials and what constitutes a legitimate educational interest. The LEA will provide parents with a notice of the websites and online services under this agreement for which it has consented to student data collection to on behalf of the parent, as permitted under COPPA

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 Virginia and Federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRA, Code of Virginia § 22.1-289.01. and § 22.1-287.02.

2. **Authorized Use**. Student Data shared pursuant to this DPA, including persistent unique identifiers, shall be used for no purpose other than the Services stated in this DPA and as authorized under the statutes referred to in subsection (1), above. Provider also acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, any Student Data, metadata, 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, or there is a court order or lawfully issued subpoena for the information.

3. **Employee Obligations**. 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 the Service Agreement.

4. **Use of De-identified Information**. De-identified information, as defined in Exhibit "C", 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 CFR 99.31(b). The Provider and LEA agree

that the Provider cannot successfully de-identify information if there are fewer than twenty (20) students in the samples of a particular field or category of information collected, i.e., twenty students in a particular grade, twenty students of a particular race, or twenty students with a particular disability. Provider agrees not to attempt to re-identify de-identified Student Data and not to transfer de-identified Student Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to the LEA who has provided prior written consent for such transfer.

5. **Disposition of Data**. Upon written request and in accordance with the applicable terms in subsections below, provider shalt dispose or delete all Student data obtained under this agreement when it is no longer needed for the purposes for which it was obtained. Disposition will include (1) the shredding of any hard copies 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 digital means. Nothing in the service agreement authorizes provider to maintain Student data obtained under the service agreement beyond the time reasonably needed to complete the disposition. Provider shall provide written notification 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 terms of the agreement. The LEA may employ a request for return or deletion of Student data form, a copy of which is attached hereto as exhibit D. Upon receipt of a request from the LEA, the provider will immediately provide the LEA with any specified portion of the Student data within fourteen (14) calendar days of the receipt of said request.

   a. **Partial Disposal During the Term of Service Agreement**. Throughout the term of the service agreement, LEA may request partial disposal of Student data obtained under the service agreement that is no longer needed. Partial disposal of data shall be subject to LEA's request to transfer data to a separate account, pursuant to Article II Section 3, above.

   b. **Complete Disposal upon Termination of Service Agreement**. Upon termination of the service agreement provider shall dispose or securely destroy all Student data obtained under the service agreement. Prior to disposal of the data, provider shall notify LEA in writing of it option to transfer data to a separate account, pursuant to Article 2, Section 3, above. In new event shelters provider dispose of data pursuant to this provision unless and until provider has received affirmative written confirmation from LEA that data will not be transferred to a separate account.

   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 families/guardians; (b) inform, influence, or enable marketing or advertising 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 Client; or (d) use the Student Data for the development of commercial products or services, other than as necessary to provide the Service to Client. This section does not prohibit Provider from generating legitimate personalized learning recommendations or other activities permitted under Code of Virginia § 22.1-289.01.
7. **Penalties.** The failure to comply with the requirements of this agreement could subject Provider and any third party to all allowable penalties assessable against Provider under

state and federal law. In the event the Family Policy Compliance Office of the U.S. Department of Education determines that Provider improperly disclosed personally identifiable information obtained from the Student's education records, the LEA may not allow Provider access to the LEA's education records for at least five years.

ARTICLE V: DATA PROVISIONS

1. **Data Security**. The Provider agrees to maintain a comprehensive information security program that is reasonably designed to protect the security, privacy, confidentiality, and integrity of student personal information and makes use of appropriate administrative, technological, and physical safeguards. The general security duties of Provider are set forth below. These duties shall include, but are not limited to:
   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.

   a. **Security Protocols**. Both parties agree to maintain security protocols that meet industry best practices in the collection, storage 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 DPA in a secure computer environment.

   b. **Provider Employee Training**. The Provider shall provide annual security training to those of its employees who operate or have access to the system.

   c. **Security Technology**. When the service is accessed using a supported web browser, FIPS 140-2 validated transmission encryption protocols, or equivalent technology shall be employed to protect data from unauthorized access. The service security measures shall follow National Institute of Standards and Technology (NIST) 800- 171, or equivalent industry best practices.

   d. **Periodic Risk Assessment**. Provider further acknowledges and agrees to conduct periodic risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner. Upon LEA's written request, Service Provider shall make the results of findings available to the LEA. The LEA shall treat such audit reports as Provider's Confidential Information under this Agreement.

   e. **Backups and Audit Trails, Data Authenticity and Integrity**. Provider will take reasonable measures, including all backups and audit trails, to protect

Student Data against deterioration or degradation of data quality and authenticity. Provider shall be responsible for ensuring that Student Data is retrievable in a reasonable format.

f. **Subprocessors Bound**. Provider shall enter into written agreements whereby Subprocessors agree to secure and protect Student Data in a manner consistent with the terms of this Article V. Provider shall periodically conduct or review compliance monitoring and assessments of Subprocessors to determine their compliance with this Article.

2. **Unauthorized Access or Data Breach**. In the event that Student Data are reasonably believed by the Provider or school division to have been disclosed (lost, accessed or obtained) in violation of the Family Educational Rights and Privacy Act (20 U.S.C. § 1232g) or other federal or state law
applicable to such information accessed or obtained by an unauthorized individual, Provider shall follow the following process:

a. provide immediate notification to LEA upon verification of the incident and allow the LEA or its authorized representatives to fully participate in the investigation of the incident.

b. notification will be provided to the contact(s) identified in ARTICLE VII, N: Notice, and sent via email and postal mail. Such notification shall include the

i. date, estimated date, or date range of the loss or disclosure;
ii. Student Data that was or is reasonably believed to have been lost or disclosed;
iii. remedial measures taken or planned in response to the loss or disclosure.

c. immediately take action to prevent further access;
d. take all legally required, reasonable, and customary measures in working with LEA to remediate the breach, which may include toll free telephone support with informed customer services staff to address questions by affected parties and/or provide monitoring services if necessary given the nature and scope of the loss or disclosure;
e. cooperate with LEA efforts to communicate to affected parties.
f. provider is prohibited from directly contacting parent, legal guardian or eligible pupil unless expressly requested by LEA. If LEA requests Provider's assistance providing notice of unauthorized access, and such assistance is not unduly burdensome to Provider, Provider shall notify the affected parent, legal guardian or eligible pupil of the unauthorized access, which shall include the information listed in subsections (b) and (c), above. If requested by LEA, Provider shall reimburse LEA for costs incurred to notify parents/families of a breach not originating from LEA's use of the Service, but only in proportion to and to the extent such liabilities are caused by the negligence, recklessness, willful misconduct or internal acts, omissions of Provider
g. the Provider shall hold harmless the LEA from and against any loss, claim, cost (including attorneys' fees) or damage of any nature arising from or in connection with the breach by the Provider or any of its officers, directors, employees, agents or representatives of the obligations of the Provider’s or

its Authorized Representatives under this provision or under a Confidentiality Agreement, as the case may be.

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. **Data Transfer Upon Termination or Expiration**. Provider will notify the LEA of impending cessation of its business and any contingency plans. Provider shall implement its exit plan and take all necessary actions to ensure a smooth transition of service with minimal disruption to the LEA. As mutually agreed upon and as applicable, Provider will work closely with its successor to ensure a successful transition to the new equipment, with minimal downtime and effect on the Division, all such work to be coordinated and performed in advance of the formal, transition date.

4. **Effect of Termination Survival. I**f the DPA is terminated, the Provider shall destroy all of Student's data pursuant to Article V, section 5(b). The Provider's obligations under this agreement shall survive termination of this Agreement until all Division Data has been returned or Securely Destroyed.

5. **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.

6. . **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 or 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.

7. **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: **Louis McDonald**
Title: Director, Technology Services
Contact Information:
320 Hospital Dr Ste 40
Warrenton, VA
20186-3037
Email: Louis.McDonald@fcps1.org
Phone Number: 540-422-7013

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

8. **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.

9. **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.

10. **Governing Law: Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF VIRGINIA, 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.

11. **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.

12. **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.

13. **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.

14. **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.

15. **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 Virginia Student Data Privacy Agreement as of the last day noted below.

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

BY: _____ Date: 25-Mar-2020

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

Fauquier County Public School District

BY: Louis McDonald Date: 25-Mar-2020

Printed Name: **Louis McDonald** Title/Position: **Director, Technology Services**

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 schedule d courses	
	Teacher names	
Special Indicator	English language learner information	
	Low income status	
	Medical alerts/health data	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information – 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

Data Breach means an event in which Division Data is exposed to unauthorized disclosure, access, alteration or use.

LEA Data includes all business, employment, operational and Personally Identifiable Information that Division provides to Provider and that is not intentionally made generally available by the LEA on public websites or publications, including but not limited to business, administrative and financial data, intellectual property, and student, employees, and personnel data, user generated content and metadata but specifically excludes Provider Data (as defined in the Contract).**De-Identifiable Information (DII):** De-Identification refers to the process by which the Provider removes or obscures any Personally Identifiable Information ("PII") from student records in a way that removes or minimizes the risk of disclosure of the identity of the individual and information about them. Anonymization or de-identification should follow guidance equivalent to that provided by U.S Department of Education publication "Data De-identification: An Overview of Basic Terms" or NISTIR Special Publication (SP) 8053 De-Identification of Personally Identifiable Information. The Provider's specific steps to de-identify the data will depend on the circumstances but should be appropriate to protect students. Some potential disclosure limitation methods are blurring, masking, and perturbation. De-identification should ensure that any information when put together cannot indirectly identify the student, not only from the viewpoint of the public, but also from the vantage of those who are familiar with the individual. Information cannot be de- identified if there are fewer than twenty (20) students in the samples of a particular field or category, i.e., twenty students in a particular grade or less than twenty students with a particular disability.

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.

Indirect Identifiers: Any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty

Personally Identifiable Information (PII): The terms "Personally Identifiable Information" or "PII" shall include, but are not limited to, student data, staff data, parent 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 Division or its users, students, or students' parents/guardians, including "directory information" as defined by §22.1-287.1 of the Code of Virginia".

PII includes, without limitation, at least the following:

- Staff, Student or Parent First, Middle and Last Name
- Staff, Student or Parent Telephone Number(s)
- Discipline Records
- Special Education Data
- Grades
- Criminal Records
- Health Records
- Biometric Information
- Socioeconomic Information
- Political Affiliations
- Text Messages
- Student Identifiers Photos
- Videos
- Grade
- Home Address Subject
- Email Address
- Test Results
- Juvenile Dependency Records Evaluations
- Medical Records
- Social Security Number
- Disabilities
- Food Purchases
- Religious Information Documents
- Search Activity
- Voice Recordings
- Date of Birth
- Classes
- Information in the Student's Educational Record
- Information in the Student's Email

Provider: For purposes of the DPA, the term "Provider" means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of 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 Division 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 local educational employee.

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.
Securely Destroy: Securely Destroy: Securely Destroy means taking actions that render data written on physical (e.g., hardcopy, microfiche, etc.) or electronic media unrecoverable by both

ordinary and extraordinary means. These actions must meet or exceed those sections of the National Institute of Standards of Technology (NIST) SP 800-88 Appendix A guidelines relevant to sanitization of data categorized as high security. All attempts to overwrite magnetic data for this purpose must utilize DOD approved methodologies.

School Official: For the purposes of this Agreement and pursuant to 34 CFR 99.31 (B), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of education records; and (3) Is subject to 34 CFR 99.33(a) governing the use and re-disclosure of personally identifiable information from student records.

Student Data: Student Data includes any data, whether gathered by Provider or provided by Division or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, home address, telephone number, email address, or other information allowing online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information text messages, documents, student identifies, search activity, photos, voice recordings or geolocation information.

Student Data shall constitute Pupil Records for the purposes of this Agreement, and for the purposes of Virginia and Federal laws and regulations. Student Data as specified in Exhibit B is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services. Anonymization or de-identification should guidance equivalent to that provided by U.S Department of Education publication "Data De-identification: An Overview of Basic Terms" or NISTIR Special Publication (SP) 8053 De-Identification of Personally Identifiable Information.

Student Generated Content: Alternatively known as user-created content (UCC), is any form of content, such as images, videos, text and audio, that have been created and posted by student users on online platforms.

Subscribing LEA: An LEA that was not party to the original Services Agreement and who accepts the Provider'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 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.

Third Party: The term "Third Party" means an entity that is not the Provider or LEA.

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 (d/b/a Lightspeed Systems), (hereinafter referred to as "Provider"), offers the same privacy protections found in this DPA between it and Fauquier County Public School District , (hereinafter referred to as the "LEA") and which is dated 25-Mar-2020

, 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: 25-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: John Genter

Title: VP, Global Operations

Email Address: privacy@lightspeedsystems.com

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 Ye**s □ No

   - If yes, please provide it.
   - Upon signing a non-disclosure agreement 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
__**x** __CIS Critical Security Controls
__**x**__NIST Framework for Improving Critical Infrastructure Security
__**x**__ Other: **NIST Privacy framework 1.0** _ _____

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

6. List of Providers Sub-processors
   a. Upon signing a non-disclosure agreement, LEA may be provided a copy of the Providers Sub-processors