

UTAH STUDENT DATA PRIVACY AGREEMENT

Version 2.0

Washington County School District

and

Lightspeed Systems

Date 22-Apr-2020

This Utah Data Privacy Agreement (“DPA”) is entered into by and between the **Washington 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 22-Apr-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 educational services (“Services”) pursuant to a contract dated (“Service Agreement”); 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 Educational Rights and Privacy Act (“FERPA”) at 20 U.S.C. 1232g (34 CFR Part 99), Children’s Online Privacy Protection Act (“COPPA”), 15 U.S.C. 6501-6506; 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 Utah state student privacy laws, including the Utah Student Data Protection Act UCA Section 53E-9; and

WHEREAS, for the purposes of this DPA, Provider is a school official with legitimate educational interests in accessing Education Records pursuant to the Service Agreement for the limited purposes of this DPA; 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 Utah 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, COPPA, PPRA and other applicable Utah 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, and performing services otherwise provided by the LEA. With respect to the use and maintenance of Student Data, Provider shall be under the direct control and supervision of the LEA.

2. **Nature of Services Provided.** The Provider has agreed to provide digital educational products and services outlined in Exhibit "A".

3. **Student Data to Be Provided.** The Parties shall indicate the categories of student data to be provided in the Schedule of Data, attached 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 the student.

2. **Parent Access.** The LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may request the opportunity to inspect and review Student Data in the student's records, and seek to amend Student Data that are inaccurate, misleading or in violation of the student's right of privacy. Provider shall respond in a timely manner (and no later than 45 days from the date of the request) to the LEA's request for Student Data in a student's records held by the Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.

3. **Third Party Request.** Should a Third Party, including law enforcement and government entities, request data held by the Provider pursuant to the Services Agreement, the Provider shall redirect the Third Party to request the data directly from the LEA. Provider shall notify the LEA in advance of a compelled disclosure to a Third Party. Provider shall share Student Data with law enforcement if required by law or court order.

4. **Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner consistent with the terms of this DPA. Provider shall provide the LEA with a description of the subprocessors or types of subprocessors who have access to the LEA's student data and shall update the list as new subprocessors are added.

ARTICLE III: 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 and all other Utah privacy statutes as they relate to the collection, use, storage, or sharing of student data.

2. **Authorized Use.** The data shared pursuant to the Service Agreement, including persistent

unique identifiers, shall be used for no purpose other than the Services stated in the Service Agreement and/or otherwise authorized under the statutes referenced in the prior subsection. Provider also acknowledges and agrees that it shall not make any re-disclosure of any Student Data.

3. Employee Obligation. Provider shall require all employees and subprocessors 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 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). Provider agrees not to attempt to re-identify de-identified Student Data.

5. Disposition of Data. Upon written request 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. The duty to dispose of Student Data shall not extend to data that has been de-identified. 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 14 calendar days of receipt of said request.

- a. **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. Additional Acceptable Uses of Student Data. Provider is prohibited from using Student Data for any secondary use not described in this agreement except:

- a. for adaptive learning or customized student learning purposes;
- b. to market an educational application or product to a parent or legal guardian of a student if Provider did not use Data, shared by or collected per this Contract, to market the educational application or product;
- c. to use a recommendation engine to recommend to a student
 - i. content that relates to learning or employment, within the third-party Provider's internal application, if the recommendation is not motivated by payment or other consideration from another party; or
 - ii. services that relate to learning or employment, within the third-party Provider's internal application, if the recommendation is not motivated by payment or other consideration from another party;
- d. to respond to a student request for information or feedback, if the content of the response is not motivated by payment or other consideration from another party.; and
- e. to use Data to allow or improve operability and functionality of the third-party Provider's internal application. _

ARTICLE IV: DATA PROVISIONS

1. Data Security. The Provider agrees to abide by and maintain adequate data security measures, consistent with standards and best practices within the educational technology industry, and to protect Student Data from unauthorized disclosure or acquisition by an unauthorized person. These measures shall include, but are not limited to:

- a. Passwords and Employee Access.** Provider shall secure usernames, passwords, and any other means of gaining access to the Services or to Student Data. Provider shall only provide access to Student Data to employees or Providers that are performing the Services.
- b. Security Protocols.** Both parties agree to maintain security protocols that meet industry standards in the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. 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.
- c. Security Technology.** Provider shall employ internet industry standard measures to protect data from unauthorized access while the data is in transit or at rest. 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.
- d. Audit Rights.** Upon reasonable notice, and at the request of the LEA, the LEA or the LEA's designee may audit the Provider, at the LEA's expense, to verify compliance with this DPA, as required by the Utah Student Data Protection Act. The LEA shall treat such audit reports as Provider's Confidential Information under this Agreement.

2. Data Breach. In the event that Provider discovers that Student Data has been accessed or obtained by an unauthorized individual, Provider shall provide notification to LEA within a reasonable amount of time of the incident, not to exceed 72 hours.

ARTICLE V- GENERAL OFFER OF PRIVACY TERMS

Provider may, by signing the attached Form of General Offer of Privacy Terms in Exhibit "E", be bound by the terms of this DPA to any other LEA who signs the acceptance on in said Exhibit.

ARTICLE VI: 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 so long as the Service Agreement has lapsed or has been terminated. LEA shall have the right to terminate the DPA and Service Agreement in the event of a material breach of the terms of this DPA.
3. **Effect of Termination Survival**. If the Service Agreement is terminated, the Provider shall destroy all of LEA's data pursuant to Article III, section 5 above.
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 paragraph herein, all other provisions of the Service Agreement shall remain in effect.
5. **Notice**. All notices or other communication required or permitted to be given hereunder must be in writing and given by personal delivery, 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: Marsha Langland
Title: Digital Learning Facilitator

Contact Information:
marsha.langland@washk12.org
934 S 100 E
ST GEORGE, UT 84770-7432

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 given 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.

The designated representative for notice of acceptance of the General Office 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

6. 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.

7. Severability. Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.

8. Governing Law; Venue and Jurisdiction. THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF UTAH, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS OF UTAH FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS SERVICE AGREEMENT OR THE TRANSACTIONS CONTEMPLATED HEREBY.

9. Authority. Provider represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or Providers 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 portion thereof stored, maintained or used in any way. Provider agrees that any purchaser of the Provider shall also be bound to this DPA.

10. 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. LEA hereby waives and releases any and all claims against the Utah State Board of Education and/or its members, departments, office, and staff (collectively, "USBE"), for USBE's efforts and conduct related to the negotiations and/or formation of this DPA. The parties agree that USBE is not an agent nor a representative of LEA in the formation or execution of this DPA, and that LEA negotiated with Provider at arm's length in the creation of this DPA. USBE is thus not responsible or liable to either party under this DPA, and owes no duty to either party under this DPA.

11. Successors Bound. This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business.

12. 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.

13. 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 Utah Student Data Privacy Agreement as of the last day noted below.

Lightspeed Solutions LLC (d/b/a Lightspeed Ssystems)

BY:  Date: 22-Apr-2020

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

Washington County School District

BY: Larry Bergeson Date: 22-Apr-2020

Printed Name: Larry Bergeson Title/Position: Superintendent

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 STUDENT DATA

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

Category of Data	Elements	Check if used by your system	Category of Data	Elements	Check if used by your system
	to link parents to students)			number	
				State ID number	
Parent/Guardian Name	First and/or Last			Vendor/App assigned student ID number	
				Student app username	
Schedule	Student scheduled courses			Student app passwords	
	Teacher names				
			Student Name	First and/or Last	X
	English language learner information				
	Low income status		Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	
	Medical alerts /health data				
	Student disability information		Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Special Indicator	Specialized education services (IEP or 504)				
	Living situations (homeless/foster care)		Student Survey Responses	Student responses to surveys or questionnaires	
	Other indicator information- Please specify:				
Student Contact Information	Address				
	Email	X			
	Phone		Student work	Student generated content; writing, pictures etc.	
				Other student work data -	
Student Identifiers	Local (School district) ID	X			

Category of Data	Elements	Check if used by your system
	Please specify:	
Transcript	Student course grades	
	Student course data	
	Student course grades/performance scores	
	Other transcript data -Please specify:	
Transportation	Student bus assignment	
	Student pick up and/or drop off location	
	Student bus card ID number	
	Other transportation data -Please specify:	
Other	Please list each additional data element used, stored or collected by your application	X

No Student Data Collected at this time_____.

*Provider shall immediately notify LEA if this designation is no longer applicable.

OTHER: Use this box, if more space 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

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 Provider” as used in the Student Data Protection Act and “Operator” as used in COPPA.

De-Identified Information (DII): De-Identification refers to the process by which the Provider removes or obscures any Personally Identifiable Information (“PII”) from Education Records in a way that removes or minimizes the risk of disclosure of the identity of the individual and information about them.

Education 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, Education Records are referred to as Student Data.

Personally Identifiable Information (PII): The terms “Personally Identifiable Information” or “PII” has the same meaning as that found in U.C.A § 53E-9-301, and includes both direct identifiers (such as a student’s or other family member’s name, address, student number, or biometric number) and indirect identifiers (such as a student’s date of birth, place of birth, or mother’s maiden name). Indirect identifiers that constitute PII also include metadata or other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty. For purposes of this DPA, Personally Identifiable Information shall include the categories of information listed in the definition of Student Data.

Student Generated Content: The term “student-generated content” means materials or content created by a student 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 student content.

R277-487, Public School Data Confidentiality and Disclosure: The implementing Rule authorized by Utah Constitution Article X, Section 3, which vests general control and supervision over public education in the Board, and further authorizes the Board to make rules to establish student data protection standards for public education, pursuant to Subsection 53E-9- 302(1) of the Utah Student Data Protection Act.

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

and modifies.

School Official: For the purposes of this Agreement and pursuant to 34 CFR 99.31 (B), a School Official is a Provider 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.

Student Data: Student Data means personally identifiable information, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, 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 Education Records for the purposes of this Agreement, and for the purposes of Utah 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.

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 "SubProvider") 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: means presenting advertisements to a student where the advertisement is selected based on information obtained or inferred over time from that student's online behavior, usage of applications, or student data. Targeted advertising does not include advertising to a student (i) at an online location based upon that student's current visit to that location; or (ii) in response to that student's request for information or feedback, without retention of that student's online activities over time for the purpose of targeting subsequent ads.

Utah Student Data Protection Act (Utah Title 53E-9-301 through 53E-9-310): Means the applicable Utah regulations regarding student data, as further implemented by the Superintendent pursuant to R277-487.

EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF STUDENT DATA

[Name or District or LEA] directs [Name of Provider] 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:

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

Authorized Representative of LEA

Date

Verification of Disposition of Data
by Authorized Representative of Provider

Date

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 Washington County School District and which is dated 22-Apr-2020 to any other LEA ("Subscribing LEA") who accepts this General Offer though 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: (1) a material change in the applicable privacy statutes; or (2) a material change in the services and products subject listed in the Originating Service Agreement. Provider shall notify the Utah State Board of Education (privacy@schools.utah.gov) in the event it withdraws Exhibit E so that the withdrawal may be disseminated to the LEAs.

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

BY: 

Date: 22-Apr-2020

Printed Name: Greg 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? **Yes** **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
 CIS Critical Security Controls
 NIST Framework for Improving Critical Infrastructure Security
 Other: **NIST Privacy framework 1.0** _ _____

3. Does your organization store any customer data outside the United States?
 Yes **No**
4. Does your organization encrypt customer data both in transit and at rest? **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