

CALIFORNIA STUDENT DATA PRIVACY AGREEMENT
Version 1.0

Bass Lake Joint Union Elementary SD

and

ExploreLearning, LLC

Reflex

11/07/2018

This California Student Data Privacy Agreement ("DPA") is entered into by and between the Bass Lake Joint Union Elementary SD (hereinafter referred to as "LEA") and ExploreLearning, LLC (hereinafter referred to as "Provider") on The Parties agree to the 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 11/07/2018 ("Service Agreement"); and

WHEREAS, in order to provide the Services described in the Service Agreement, the Provider may receive and the LEA may provide documents or data that are covered by several federal and statutes, among them, the Family Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. 1232g, Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. 6501- 6502; Protection of Pupil Rights Amendment ("PPRA") 20 U.S.C. 1232 h; and

WHEREAS, the documents and data transferred from California LEAs are also subject to several California student privacy laws, including AB 1584, found at California Education Code Section 49073.1 and the Student Online Personal Information Protection Act (sometimes referred to as either "SB 1177" or "SOPIPA") found at California Business and Professions Code section 22584; 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", agrees to allow other LEAs in California 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 the LEA pursuant to the Service Agreement, including compliance with all applicable privacy statutes, including the FERPA, PPRA, COPPA, SB 1177 (SOPIPA), and AB 1584. 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. Provider shall be under the direct control and supervision of the LEA. Control duties are set forth below.
2. **Nature of Services Provided.** The Provider has agreed to provide the following digital educational services described below and as may be further outlined in Exhibit "A" hereto:

Use of the Reflex. ExploreLearning Reflex®, the most powerful solution available for math fact fluency. Reflex is adaptive and individualized. Reflex continuously monitors each student's performance to create the optimal experience for every child. Reflex includes intuitive and powerful reporting. Educators have everything they need to easily monitor and support student progress. Reflex is game-based to keep students coming back for more.

3. **Student Data to Be Provided.** In order to perform the Services described in the Service Agreement, LEA shall provide the categories of data described below or as indicated 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 or any other Pupil Records 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 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 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 LEAs as it pertains to the use of student data notwithstanding the above. 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 by which a parent, legal guardian, or eligible student may review personally identifiable information on the pupil's records, correct erroneous information, and procedures for the transfer of pupil-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner 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 request of the LEA, transfer Student generated content to a separate student account.
4. **Third Party Request.** Should a Third Party, including law enforcement and government entities, contact Provider with a request for data held by the Provider pursuant to the Services, 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 unless legally prohibited.

5. ~~Unauthorized~~ Provider shall not disclose Student Data or information in a Pupil Record for any purpose other than the Service Agreement.

6. ~~Subprocessors~~ Provider shall enter into written agreements with all Subprocessors performing functions on its behalf, whereby the Subprocessors agree to protect Student Data in accordance with the terms of this DPA.

III: DUTIES OF LEA

1. ~~Provide Data~~ LEA shall provide data for the purposes of the Service Agreement in accordance with the Family Educational Rights and Privacy Act ("FERPA"), 20 U.S.C. 1232, and any other applicable privacy statutes quoted in this DPA.

2. ~~Reasonable~~ Provider shall take reasonable precautions to secure usernames, passwords, and any other information used to access the services and hosted data.

3. ~~Unauthorized~~ Provider shall notify LEA promptly of any known or suspected unauthorized access to or use of Student Data by Provider in any efforts by Provider to investigate and respond to any unauthorized access.

4. ~~District Representative~~ Provider, LEA shall designate an employee or agent of the District as the District Representative for the coordination and fulfillment of the duties of this DPA.

IV: DUTIES OF PROVIDER

1. ~~Privacy Compliance~~ Provider shall comply with all California and Federal laws and regulations pertaining to the protection of Student Data, including FERPA, COPPA, PPRRA, AB 1584, and SOPIPA.

2. ~~Authorized Use~~ Provider shall not use Student Data for any purpose other than the Services stated in the Service Agreement, unless otherwise authorized in writing by LEA. Provider shall be bound by all applicable laws and regulations referred to in subsection (1), above.

3. ~~Employee Obligations~~ Provider shall require all employees and agents who have access to Student Data to comply with applicable provisions of FERPA laws with respect to the data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement with any employee or agent with access to Student Data pursuant to the Service Agreement.

4. ~~No Disclosure~~ Provider shall not disclose any data obtained under the Service Agreement in a manner that could identify individual student to any other entity in published results of studies as authorized by the Service Agreement. Deidentified information may be used by the vendor for the purposes of development and improvement of educational sites, services, or applications.

5. **Disposition of Data.** Provider shall dispose of all personally identifiable data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained and transfer said data to LEA or LEA's designee within 60 days of the date of termination and according to a schedule and procedure as the Parties may reasonably agree. Nothing in the Service Agreement authorizes Provider to maintain personally identifiable data obtained under the Service Agreement beyond the time period reasonably needed to complete the disposition. Disposition shall include (1) the shredding of any hard copies of any Pupil Records; (2) Erasing; or (3) Otherwise modifying the personal information in those records to make it unreadable or indecipherable. Provider shall provide written notification to LEA when the 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. Nothing in the Service Agreement authorizes Provider to maintain personally identifiable data beyond the time period reasonably needed to complete the disposition.

6. **Advertising Prohibition.** Provider is prohibited from using Student Data to conduct or assist targeted advertising directed at students or their families/guardians. This prohibition includes the development of a profile of a student, or their families /guardians or group, for any commercial purpose other than providing the service to client. This shall not prohibit Providers from using data to make product or service recommendations to LEA.

ARTICLE V: DATA PROVISIONS

1. **Data Security.** The Provider agrees to abide by and maintain adequate data security measures to protect Student Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of Provider are set forth below. Provider may further detail its security programs and measures in Exhibit "D" hereto. These measures shall include, but are not limited to:
 - a. **Passwords and Employee Access.** Provider shall make best efforts practices to secure usernames, passwords, and any other means of gaining access to the Services or to Student Data, at a level suggested by Article 4.3 of NIST 800-63-3. Provider shall only provide access to Student Data to employees or contractors that are performing the Services. As stated elsewhere in this DPA, employees with access to Student Data shall have signed confidentiality agreements regarding said Student Data. All employees with access to Student Records shall pass criminal background checks.
 - b. **Destruction of Data.** Provider shall destroy all personally identifiable 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 a schedule and procedure as the parties may reasonable agree. Nothing in the Service Agreement authorizes Provider to maintain personally identifiable data beyond the time period reasonably needed to complete the disposition.
 - c. **Security Protocols.** Both parties agree to maintain security protocols that meet industry best practices in the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. Provider shall maintain all data obtained or generated pursuant to the Service Agreement in a secure computer 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 periodic security training to those of its employees who operate or have access to the system. 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, Secure Socket Layer ("SSL"), or equivalent technology protects information, using both server authentication and data encryption to help ensure that data are safe secure only to authorized users. Provider shall host data pursuant to the Service Agreement in an environment using a firewall that is periodically updated according to industry standards.
 - f. **Security Coordinator.** Provider shall provide the name and contact information of Provider's Security Coordinator for the Student Data received pursuant to the Service Agreement
 - g. **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. **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. Provider shall follow the following process:
- a. The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described herein under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.
 - b. The security breach notification described above in section 2(a) shall include, at a minimum, the following information:
 - i. The name and contact information of the reporting LEA subject to this section.
 - ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
 - iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
 - iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.
 - v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
 - c. At LEA's discretion, the security breach notification may also include any of the following:
 - i. Information about what the agency has done to protect individuals whose information has been breached.
 - ii. Advice on steps that the person whose information has been breached may take to protect himself or herself.

- d. Any agency that is required to issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. Provider shall assist LEA in these efforts.
- e. At the request and with the assistance of the District, 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.

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. 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. Notwithstanding the foregoing, Provider agrees to be bound by the terms and obligations of this DPA for no less than three (3) years.
2. **Termination.** In the event that either party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated.
3. **Effect of Termination Survival.** If the Service Agreement is terminated, the Provider shall destroy all of the LEA's data pursuant to Article V, section 1(b).
4. **Priority of Agreements.** This DPA shall govern the treatment of student records in order to comply with the privacy protections, including those found in FERPA and AB 1584. In the event there is conflict between the terms of the DPA and the Service Agreement, or with any other bid/RFP, license agreement, or writing, the terms of this 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, 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 addresses set forth herein.
6. **Application of Agreement to Other Agencies.** Provider may agree by signing the General Offer of Privacy Terms be bound by the terms of this DPA for the services described therein for any Successor Agency who signs a Joinder to this DPA.

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.

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 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.

9. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF CALIFORNIA,

WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES, EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS LOCATED IN MADERA COUNTY, CALIFORNIA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS SERVICE AGREEMENT OR THE TRANSACTIONS CONTEMPLATED HEREBY.

[Signature Page Follows]

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

Bass Lake Joint Union Elementary SD

Signature: 

Date: 11-19-2018

Printed Name: RANDALL M. SEACS

Title/Position: SUPERINTENDENT

ExploreLearning, LLC
Reflex

Signature: 

Date: 11/7/18

Printed Name: DAVID SUSTER

Title/Position: PRESIDENT

Note: Electronic signature not permitted.

EXHIBIT "A"
DESCRIPTION OF SERVICES

Use of the Gizmos product. Gizmos are interactive math and science simulations for grades 3-12. Over 400 Gizmos aligned to the latest standards help educators bring powerful new learning experiences to the classroom. Gizmos use an inquiry-based approach to learning that has been validated by extensive research as a highly effective way to build conceptual understanding.

Use of the Reflex. ExploreLearning Reflex®, the most powerful solution available for math fact fluency. Reflex is adaptive and individualized. Reflex continuously monitors each student's performance to create the optimal experience for every child. Reflex includes intuitive and powerful reporting. Educators have everything they need to easily monitor and support student progress. Reflex is game-based to keep students coming back for more.

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:	
Application Use Statistics	Meta data on user interaction with application	X
Assessment	Standardized test scores	
	Observation data	X
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications that are captured (emails, blog entries)	
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	Place of Birth	
	Gender	X
	Ethnicity or race	X
	Language information (native, preferred or primary language spoken by student)	X
	Other demographic information-Please specify:	
Enrollment	Student school enrollment	X
	Student grade level	X
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information-Please specify:	
Parent/Guardian Contact Information	Address	
	Email	X
	Phone	
Parent/Guardian ID	Parent ID number (created to link parents to students)	
Parent/Guardian Name	First and/or Last	

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

Category of Data	Elements	Check if used by your system
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	

EXHIBIT "C"
DEFINITIONS

AB 1584, Buchanan: The statutory designation for what is now California Education Code § 49073. 1, relating to pupil records.

De-Identifiable Information (DI): De-Identification refers to the process by which the Vendor 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.

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

Operator: For the purposes of SB 11 77, SOPIPA, 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 AB 1584.

Personally Identifiable Information (PII): The terms "Personally Identifiable Information" or "PII" shall include, but are not limited to, student 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, without limitation, at least the following:

First and Last Name	Home Address
Telephone Number	Email Address T
Discipline Records	Test Results
Special Education Data	Juvenile Dependency
Grades	Records Evaluations
Criminal Records	Medical Records
Health Records	Social Security Number
Biometric Information	Disabilities
Socioeconomic	Food Purchases
Information Political	Religious Information
Affiliations	Documents
Text Messages Student	Search Activity
Identifiers Photos	Voice Recordings
Videos	

General Categories:

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
Information in the Student's Educational Record

Information in the Student's Email

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 Service Agreement the term "Provider" replaces the term "Third Party as defined in California Education Code § 49073.1 (AB 1584, Buchanan), and replaces the term as "Operator" as defined in SB 1177, SOPIPA.

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 local educational LEA employee.

SB 1177, SOPIPA: Once passed, the requirements of SB 1177, SOPIPA were added to Chapter 22.2 (commencing with Section 22584) to Division 8 of the Business and Professions Code relating to privacy.

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 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 CFR 99.33(a) governing the use and redisclosure of personally identifiable information from student records.

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, 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 California 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 "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 PU.

This term shall also include in its meaning the term "Service Provider," as it is found in SOPIPA.

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.

Third Party: The term "Third Party" as appears in California Education Code § 49073.1 (AB 1584, Buchanan) 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"
DATA SECURITY REQUIREMENTS

N/A

A committee of management and confidential employees met to review past year's compensation packages and discuss recommendations for this coming 2019-2020 year. The committee consisted of Dan Borgen, Gabe De La O, Pauline Elders, Nancy Lavrusky, Derrick Lawson, Allan Lehmann, and Barbara Sasser. The committee reviewed the medical plans being presented to the district from its current medical administrator, California's Valued Trust (CVT), and the newly marketed Self-Insured Schools of California (SISC) program.

SISC is offering Anthem PPO and HMO plans along with Kaiser. There is a maximum of six medical plans that an employee group may chose. This will decrease our group's plan from 11 plans to six. There is a substantial savings in the medical plans being offered compared to our 2019-2020 renewal with CVT. Our two bargaining units are currently presenting the benefits information to its members and will have a decision as to staying with CVT or moving to SISC by the first week of June.

With the management/confidential/trustee group being as small as it is, we would not cost effectively be able to stay in a program that was not attached to at least one of the bargaining units. However, the belief at this time is that both unions will move to the SISC program. Thus wanting to use the savings in other ways during negotiations.

Our main concern for the health benefits occurred a few years ago when after always following Board Policy #4154, which states in part, "Benefits for employees who are not in bargaining units shall be the same unless otherwise specific in Board policy or individual contract." Back in 2015/2016 management's medical plan district contribution stopped following classified's district contribution and remained at a standstill. Currently, classified's medical district contribution is \$15,243.96 compared to management's contribution of \$14,774.52. The committee is requesting the Board review the district's contribution towards our medical plans and have it run consistently with classifieds contribution as it allows it to do so by Board policy.

As you know, the District began offering its management and certificated groups a Tax Sheltered Annuity (TSA). Since 2011/2012 until 2018/2019 the certificated TSA has increased 38.14% from \$5,264.04 to \$7,272.00. This year's certificated TSA is scheduled to move up to a minimum of \$7,446.00. However, during all these years, the management's TSA has never increased and remains at \$7,500.00. The committee is requesting the TSA be increased to match some of the movement that certificated has enjoyed throughout the years. This would affect 13 management/confidential/trustee members.

DISTRICT POSITIONS	Desert Sands USD					Palm Springs USD				
	Range	Salary	# of steps	Duty Days	ADA	Range	Salary	# of steps	Duty Days	ADA
Chief Innovation and Information Officer	30	\$10,187 - \$13,680	7	228	29,000	42	\$9,327.60 - \$13,846.86	9		22,500
Director of Facilities Services	28	\$9,249 - \$12,387	7	228	29,000	43	\$9,560.49 - \$14,182.06	9		22,500
Director of Fiscal Services	30	\$10,187 - \$13,680	7	228	29,000	41	\$9,098.63 - \$13,508.24	9		22,500
Director of Foundation	27	\$9,605 - \$11,920	7	228	29,000			9		
Director of Graphic Services	26	\$8,388 - \$11,233	7	228	29,000					
Director of Maintenance, Operation & Transportation	28	\$8,388 - \$11,233	7	228	29,000					
Director of Nutrition Services	26	\$8,388 - \$11,233	7	228	29,000	39	\$8,661.93 - \$10,553.21	9		22,500
Director of Purchasing & Warehouse	26	\$8,388 - \$11,233	7	228	29,000	37	\$8,244.02 - \$12,238.02	9		22,500
Director of Risk Management	26	\$8,388 - \$11,233	7	228	29,000	37	\$8,244.02 - \$12,238.02	9		22,500
Director of Security and Safety Services	26	\$8,388 - \$11,233	7	228	29,000	31	\$7,109.25 - \$10,553.21	9		22,500
Director of Maintenance & Operation						41	\$9,098.63 - \$13,508.24	9		22,500
Director of Transportation Services						40	\$8,878.31 - \$13,179.54	9		22,500
Program Specialist, Special Education	25	\$8,680 - \$10,542	7	205	29,000					
Program Specialist, Mental Health,	25	\$8,680 - \$10,542	7	205	29,000					
Psychologist,	25	\$8,680 - \$10,542	7	205	29,000					
Assistant Principal, Elementary School	26	\$9,339 - \$11,341	7	210	29,000		\$97,582 - \$125,389	21	202	22,500
Assistant Principal, Middle School	26	\$9,339 - \$11,341	7	210	29,000		\$96,253 - \$127,783	21	202	22,500
Coordinator of Assessment and Accountability	26	\$9,339 - \$11,341	7	226	29,000		\$7,469.35 - \$11,086.72	9		22,500
Coordinator, Child Welfare and Attendance	26	\$9,339 - \$11,341	7	226	29,000		\$101,263 - \$128,127	21	202	22,500
Administrator of College and Career Readiness	27	\$9,805 - \$11,920	7	210	29,000					
Assistant Principal, Alternative Education	27	\$9,805 - \$11,920	7	210	29,000					
Assistant Principal, High School	27	\$9,805 - \$11,920	7	210	29,000		\$111,418 - \$142,669		215	22,500
Coordinator of Special Education	27	\$9,805 - \$11,920	7	226	29,000					
Coordinator of the Local Control Accountability Plan, Strategy & Performance	27	\$9,805 - \$11,920	7	226	29,000					
Principal, Early Childhood Education	27	\$9,805 - \$11,920	7	210	29,000					
Principal, Early Childhood Special Education	27	\$9,805 - \$11,920	7	226	29,000					
Principal, Elementary School	28	\$10,286 - \$12,506	7	210	29,000	13, 16, 17	\$111,308 - \$141,468	21	212	22,500
Director of Child Welfare and Attendance	29	\$10,802 - \$13,143	7	226	29,000					
Director of State and Federal Programs	29	\$10,802 - \$13,143	7	226	29,000					
Principal, Alternative Education	29	\$10,802 - \$13,143	7	210	29,000					
Principal, Continuation High School	29	\$10,802 - \$13,143	7	210	29,000					
Principal, Middle School	29	\$10,802 - \$13,143	7	210	29,000					
Director of Personnel, Leadership Development	29	\$10,802 - \$13,143	7	226	29,000		\$115,610 - \$145,356	21	212	22,500
Director of Professional Development and Teacher Support	29	\$10,802 - \$13,143	7	226	29,000					
Principal, Charter School	30	\$11,353 - \$13,792	7	226	29,000					
Principal, High School	30	\$11,353 - \$13,792	7	226	29,000		\$128,986 - \$164,177	21	223	22,500
Senior Director, Certificated Personnel Services and Assessment	30	\$11,353 - \$13,792	7	226	29,000					
Senior Director, Secondary Curriculum, Instruction and Assessment	30	\$11,353 - \$13,792	7	226	29,000					

\$1,300

EXHIBIT "E"
GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and Bass Lake Joint Union Elementary SD and which is dated 11/07/2018 to any other LEA ("Subscribing LEA") to any who 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 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; (2) a material change in the services and products listed in the Originating Service Agreement; or three (3) years after the date of Provider's signature to this Form. Provider shall notify the California Student Privacy Alliance in the event of any withdrawal so that this information may be transmitted to the Alliance's users.

ExploreLearning, LLC
Reflex

Signature: 

Date: 11/7/18

Printed Name: DAVID SHUSTER

Title/Position: PRESIDENT

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.

Desert Sands Unified School District

Signature: 

Date: 8/6/19

Printed Name: Jordan Aquino

Title/Position: Assistant Superintendent
Business Services

