

STANDARD STUDENT DATA PRIVACY AGREEMENT

WA-NDPA Standard

Version 1.0

**Local Education Agency (LEA):
South Kitsap School District
and**

**Provider:
YouScience, LLC**

DATE:

9/9/2021

This Student Data Privacy Agreement ("DPA") is entered into on the date of full execution (the "Effective Date") and is entered into by and between:

School District: South Kitsap School District, located at: 2669 Hoover Ave SE, Port Orchard, WA ("LEA") and
Provider: YouScience, LLC, located at: 751 Quality Dr, #200, American Fork, UT 84003 (the "Provider").

WHEREAS, the Provider is providing educational or digital services to LEA.

WHEREAS, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. § 1232g (34 CFR Part 99); the Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations and

WHEREAS, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.

NOW THEREFORE, for good and valuable consideration, LEA and Provider agree as follows:

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.
2. **Special Provisions. Check if Required.**
 - If checked, the Supplemental State Terms and attached hereto as **Exhibit "G"** are hereby incorporated by reference into this DPA in their entirety.
 - If checked, LEA and Provider agree to the additional terms of modifications set forth in **Exhibit "H"**
 - If Checked, the Provider, has signed **Exhibit "E"** to the Standard Clauses, otherwise known as General Offer of Privacy Terms
3. In the event of a conflict between the SDPC Standard Clauses, the State or Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this DPA shall control.
4. [Reserved]
5. The services to be provided by Provider to LEA pursuant to this DPA are detailed in **Exhibit "A"** (the "Services").
6. **Notices.** All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or first-class mail, sent to the designated representatives below.

The designated representative for the Provider for this DPA is:

Name: Audrey Nielsen Title: Contract & Accounting Specialist

Address: 751 Quality Dr, #200, American Fork, UT 84003

Phone: 385-273-0748 Email: audrey.nielsen@youscience.com

The designated representative for the LEA for this DPA is:

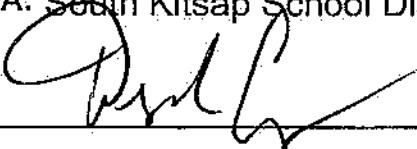
Name: Derry Lyons Title: Director of Information Technology

Address: 2689 Hoover Ave SE, Port Orchard, WA

Phone: 360-874-7030 Email: lyons@skschools.org

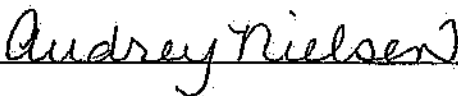
IN WITNESS WHEREOF, LEA and Provider execute this DPA as of the Effective Date.

LEA: South Kitsap School District

By:  Date: 9/9/2021

Printed Name: Derry Lyons Title/Position: Director of Information Technology

Name of Provider: YouScience, LLC

By:  Date: 9/9/20

Printed Name: Audrey Nielsen Title/Position: Contract & Accounting Specialist

STANDARD CLAUSES

Version: 3.0

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 including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, 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. Provider shall be under the direct control and supervision of the LEA, with respect to its use of Student Data.
2. **Student Data to Be Provided.** In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit "B"**.
3. **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 terms used in any other writing, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies etc.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA.** All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated 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 LEA as it pertains to the use of Student Data, notwithstanding the above.
2. **Parent Access.** To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than forty-five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) 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. **Separate Account.** If Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student-Generated Content to a separate account created by the student.
4. **Law Enforcement Requests.** Should law enforcement or other government entities ("Requesting Party(ies)") contact Provider with a request for Student Data held by the Provider pursuant to the

Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.

5. **Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws.** LEA shall provide Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.
2. **Annual Notification of Rights.** If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its annual notification of rights.
3. **Reasonable Precautions.** LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted Student Data.
4. **Unauthorized Access Notification.** LEA shall notify Provider promptly of any known unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance.** The Provider shall comply with all applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.
2. **Authorized Use.** The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in Exhibit A or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA. [See Modification at Exhibit "G"]
3. **Provider Employee Obligation.** Provider shall require all of Provider's employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Student Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.
4. **No Disclosure.** Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non-public information and/or personally identifiable information contained in the Student Data other than as directed or permitted by the LEA or this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to subprocessors performing services on

behalf of the Provider pursuant to this DPA. Provider will not Sell Student Data to any third party.

5. **De-Identified Data**: Provider agrees not to attempt to re-identify de-identified Student Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; and (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Except for Subprocessors, Provider agrees 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. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which de-identified data is presented.
6. **Disposition of Data**. Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to section II 3. The LEA may employ a "Directive for Disposition of Data" form, a copy of which is attached hereto as **Exhibit "D"**. If the LEA and Provider employ Exhibit "D," no further written request or notice is required on the part of either party prior to the disposition of Student Data described in Exhibit "D."
7. **Advertising Limitations**. Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits. [See modification at Exhibit "G"]

ARTICLE V: DATA PROVISIONS

1. **Data Storage**. Where required by applicable law, Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.
2. **Audits**. No more than once a year, or following unauthorized access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA. The Provider will cooperate reasonably with

the LEA and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA. Failure to reasonably cooperate shall be deemed a material breach of the DPA.

3. **Data Security.** The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The provider shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth set forth in **Exhibit "F"**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment to **Exhibit "H"**. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit "F"**. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.
4. **Data Breach.** In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:
 - (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:
 - 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; and
 - v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
 - (2) Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
 - (3) Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable

information and agrees to provide LEA, upon request, with a summary of said written incident response plan.

- (4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians.
- (5) In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

ARTICLE VI: GENERAL OFFER OF 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 **Exhibit "E"** 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. **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. Either party may terminate this DPA and any service agreement or contract if the other party breaches any terms of this DPA.
2. **Effect of Termination Survival.** If the Service Agreement is terminated, the Provider shall destroy all of LEA's Student Data pursuant to Article IV, section 6.
3. **Priority of Agreements.** This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between Exhibit H, the SDPC Standard Clauses, and/or the Supplemental State Terms, Exhibit H will control, followed by the Supplemental State Terms. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.
4. **Entire Agreement.** This DPA and the Service Agreement constitute 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.

5. **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.
6. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE LEA, 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 OF THE LEA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.
7. **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. In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement. The LEA has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.
8. **Authority.** Each party 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 contractors who may have access to the Student Data and/or any portion thereof.
9. **Waiver.** No delay or omission by either party to exercise any right hereunder shall be construed as a waiver of any such right and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

EXHIBIT "A"

DESCRIPTION OF SERVICES

YouScience is an online student career and personal planning system that gives students the opportunity for personal self-discovery, career exploration, and skills demonstration. The specific services provided are subject to the purchase order with the LEA. YouScience provides the student with one or more of the following services:

1. 10-year license to access YouScience Summit and certification results and/or a 3-year license to Snapshot
2. Performance measures of aptitudes and skills certifications
3. Interest survey
4. Personalized feedback
5. Career discovery
6. Resume and self-advocacy language
7. Post-secondary education research and when available, the opportunity to connect directly with post-secondary education providers
8. Local internship, work study, and employment opportunities and when available, the opportunity to connect directly with local employers

YouScience provides the faculty with one or more the following services based on the purchase order with the LEA:

1. Ability to experience the career guidance personally
2. Invitation management
3. View student results on an individual basis
4. Track student progress individually and across groups
5. Administrative reporting
6. Academic advising reporting

YouScience provides aggregated, de-identified workforce analytics.

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

Category of Data	Elements	Check if Used by Your System
Special Indicator	Teacher names	<input type="checkbox"/>
	English language learner information	<input type="checkbox"/>
	Low-income status	<input type="checkbox"/>
	Medical alerts/ health data	<input type="checkbox"/>
	Student disability information	<input type="checkbox"/>
	Specialized education services (IEP or 504)	<input type="checkbox"/>
	Living situations (homeless/foster care)	<input type="checkbox"/>
	Other indicator information-Please specify:	<input type="checkbox"/>
Student Contact Information	Address <i>ZIP code only</i>	<input checked="" type="checkbox"/>
	Email	<input checked="" type="checkbox"/>
	Phone	<input checked="" type="checkbox"/>
Student Identifiers	Local (School district) ID number	<input checked="" type="checkbox"/>
	State ID number	<input checked="" type="checkbox"/>
	Provider/App assigned student ID number	<input checked="" type="checkbox"/>
	Student app username	<input checked="" type="checkbox"/>
	Student app passwords	<input checked="" type="checkbox"/>
Student Name	First and/or Last	<input checked="" type="checkbox"/>
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	<input checked="" type="checkbox"/>
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	<input type="checkbox"/>
Student Survey Responses	Student responses to surveys or questionnaires	<input checked="" type="checkbox"/>
Student work	Student generated content; writing, pictures, etc.	<input type="checkbox"/>
	Other student work data -Please specify:	<input type="checkbox"/>
Transcript	Student course grades	<input type="checkbox"/>
	Student course data	<input type="checkbox"/>
	Student course grades/ performance scores	<input type="checkbox"/>
	Other transcript data - Please specify:	<input type="checkbox"/>
Transportation	Student bus assignment	<input type="checkbox"/>
	Students pick up and/or drop off location	<input type="checkbox"/>
	Student bus card ID number	<input type="checkbox"/>
	Other transportation data – Please specify:	<input type="checkbox"/>

Category of Data	Elements	Check if Used by Your System
Other	Please list each additional data element used, stored, or collected by your application:	<input data-bbox="1328 655 1377 705" type="checkbox"/>
None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	<input data-bbox="1328 1243 1377 1293" type="checkbox"/>

EXHIBIT "C"

DEFINITIONS

De-Identified Data and De-Identification: Records and information are considered to be de-identified when all personally identifiable information has been removed or obscured, such that the remaining information does not reasonably identify a specific individual, including, but not limited to, any information that, alone or in combination is linkable to a specific student and provided that the educational agency, or other party, has made a reasonable determination that a student's identity is not personally identifiable, taking into account reasonable available information.

Educational Records: Educational Records are records, files, documents, and other materials directly related to a student and maintained by the school or local education agency, or by a person acting for such 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.

Metadata: means information that provides meaning and context to other data being collected; including, but not limited to date and time records and purpose of creation Metadata that have been stripped of all direct and indirect identifiers are not considered Personally Identifiable Information.

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 for K–12 school purposes. Any entity that operates an internet website, online service, online application, or mobile application that has entered into a signed, written agreement with an LEA to provide a service to that LEA shall be considered an "operator" for the purposes of this section.

Originating LEA: An LEA who originally executes the DPA in its entirety with the Provider.

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 Student Data. Within the DPA the term "Provider" includes the term "Third Party" and the term "Operator" as used in applicable state statutes.

Student Generated Content: The term "student-generated content" means materials or content created by a student in the services 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.

School Official: For the purposes of this DPA 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 Student Data including 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.

Service Agreement: Refers to the Contract, Purchase Order or Terms of Service or Terms of Use.

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, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or 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, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data includes Meta Data. Student Data further includes "personally identifiable information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local 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.

Subprocessor: For the purposes of this DPA, 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 service, and who has access to Student Data.

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

Targeted Advertising: means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the operator's Internet web site, online service or mobile application by such student or the retention of such student's online activities or requests over time for the purpose of targeting subsequent advertisements. "Targeted advertising" does not include any advertising to a student on an Internet web site based on the content of the web page or in response to a student's response or request for information or feedback.

Third Party: The term "Third Party" means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Education Records and/or Student Data, as that term is used in some state statutes. However, for the purpose of this DPA, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF DATA

District or LEA: South Kitsap School District 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:

1. Extent of Disposition

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

Categories of data:

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

2. Nature of Disposition

Disposition shall be by destruction or deletion of data.

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

Special instructions: to student-owned accounts

3. Schedule of Disposition

Data shall be disposed of by the following date:

As soon as commercially practicable.

By Date:

4. Signature

Authorized Representative of LEA

Date

5. Verification of Disposition of Data

Authorized Representative of Company

Date

EXHIBIT "E"

GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and South Kitsap School District ("Originating LEA") which is dated 9/9/2021 to any other LEA ("Subscribing LEA") who accepts this General Offer of Privacy Terms ("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 Subscribing LEA may also agree to change the data provided by Subscribing LEA to the Provider to suit the unique needs of the Subscribing LEA. The Provider may withdraw the General Offer in the event of: (1) a material changes in the applicable privacy statues; (2) a material changes 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. Subscribing LEAs should send the signed **Exhibit "E"** to Provider at the following email address:

Name of Provider: YouScience, LLC

BY: Audrey Nielsen

Date: 9/9/20

Printed Name: Audrey Nielsen

Title/Position: Contract & Accounting Specialist

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 for the term of the DPA between originating LEA: South Kitsap School District and the Provider. ****PRIOR TO ITS EFFECTIVENESS, SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER PURSUANT TO ARTICLE VII, SECTION 5. ****

Name of Subscribing LEA: _____

By: _____ Date: _____

Printed Name: _____ Title/Position: _____

SCHOOL DISTRICT NAME: _____

DESIGNATED REPRESENTATIVE OF LEA:

Name: _____

Title: _____

Address: _____

Telephone Number: _____

Email: _____

EXHIBIT "F"

DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks

2/24/2020

The Education Security and Privacy Exchange ("Edspex") works in partnership with the Student Data Privacy Consortium and industry leaders to maintain a list of known and credible cybersecurity frameworks which can protect digital learning ecosystems chosen based on a set of guiding cybersecurity principles* ("Cybersecurity Frameworks") that may be utilized by Provider.

Cybersecurity Frameworks

<input type="checkbox"/>	MAINTAINING ORGANIZATION/GROUP	FRAMEWORK(S)
<input checked="" type="checkbox"/>	National Institute of Standards and Technology	NIST Cybersecurity Framework Version 1.1
<input type="checkbox"/>	National Institute of Standards and Technology	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
<input type="checkbox"/>	International Standards Organization	Information technology — Security techniques — Information security management systems (ISO 27000 series)
<input type="checkbox"/>	Secure Controls Framework Council, LLC	Security Controls Framework (SCF)
<input type="checkbox"/>	Center for Internet Security	CIS Critical Security Controls (CSC, CIS Top 20)
<input type="checkbox"/>	Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S))	Cybersecurity Maturity Model Certification (CMMC, ~FAR/DFAR)

Please visit <http://www.edspex.org> for further details about the noted frameworks.

*Cybersecurity Principles used to choose the Cybersecurity Frameworks are located here.

WA

EXHIBIT "G" – Supplemental SDPC State Terms for [State]
Version 1.0

1. Recitals shall have the following sections added: This Amendment for SDPC State Terms for Washington ("**Amendment**") is entered into on the date of full execution (the "**Effective Date**") and is incorporated into and made a part of the Student Data Privacy Agreement ("**DPA**") by and between:

School District: South Kitsap School District , located at: 2689 Hoover Ave SE, Port Orchard, WA (the "**LEA**") and
Provider Name: YouScience, LLC , located at: 751 Quality Dr, #200, American Fork, UT 84003 (the "**Provider**").

All capitalized terms not otherwise defined herein shall have the meaning set forth in the DPA.

WHEREAS, the Provider is providing educational or digital services to LEA, which services include: (a) cloud-based services for the digital storage, management, and retrieval of pupil records; and/or (b) digital educational software that authorizes Provider to access, store, and use pupil records; and

WHEREAS, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act ("**FERPA**") at 20 U.S.C. § 1232g (34 C.F.R. Part 99); the Protection of Pupil Rights Amendment ("**PPRA**") at 20 U.S.C. §1232h; and the Children's Online Privacy Protection Act ("**COPPA**") at 15 U.S.C. § 6501-6506 (16 C.F.R. Part 312), accordingly, the Provider and LEA have executed the DPA, which establishes their respective obligations and duties in order to comply with such applicable laws;

WHEREAS, the Provider will provide the services to LEA within the State of Washington and the Parties recognizes the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable Washington laws and regulations, such as the Student User Privacy in Education Rights 28.A.604 et seq. and RCW 42.56.590; and other applicable state privacy laws and regulations; and

WHEREAS, the Provider and LEA desire to enter into this Amendment for the purpose of clarifying their respective obligations and duties in order to comply with applicable Washington state laws and regulations.

NOW, THEREFORE, for good and valuable consideration, LEA and Provider agree as follows:

1. **Term**. The term of this Amendment shall expire on the same date as the DPA.
2. **Modification to Article IV, Section 2 of the DPA**. Article 4, Section 2 of the DPA is hereby amended to read as follows:

Authorized Use: The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in Exhibit "A" or stated in the Service Agreement, or authorized under the statutes referred to herein by this DPA. Provider may use or disclose data to:

- (a) Protect the security or integrity of its website, mobile application or online service.
- (b) Ensure legal or regulatory compliance or to take precautions against liability.
- (c) Respond to or participate in the judicial process.
- (d) Protect the safety of users or others on the website, mobile application or online service.
- (e) Investigate a matter related to public safety.


In undertaking the activities specified in subsections (a) through (e) above, Provider shall adhere to all applicable data protections contained in this DPA, as well as Federal and Washington State law.

3. Modification to Article IV, Section 7 of the DPA, Article IV, section 7 is hereby amended to add the following language:

(iv) providing recommendations for school, educational, or employment purposes within a school service without the response being determined in whole or in part or other consideration from a third party.

IN WITNESS WHEREOF, LEA and Provider execute this Amendment as of the Effective Date.

LEA: **South Kitsap School District**

By:  Date: 9/9/2021

Printed Name: Derry Lyons Title/Position: Director of Information Technology

Provider: **YouScience, LLC**

By:  Date: 9/9/2021

Printed Name: Audrey Nielsen Title/Position: Contract & Accounting Specialist

Exhibit "H"

DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN IS ATTACHED HERETO AND INCORPORATED HEREIN. LEA and Provider agree to the following additional terms and modifications:

YouScience Privacy Policy – refer to <https://www.youscience.com/privacy-policy/>

Last Updated: January 8, 2021

Introduction

Thank you for choosing our solutions. At YouScience:

- We value your privacy and respect your desire to keep your Personal Data private.
- We do not sell, lease, or rent your identifiable Personal Data without your explicit consent.
- We are committed to providing our Services through a secure, user-controlled environment.
- We only collect and handle Personal Data as described in our Privacy Policy.

At the same time, you share responsibility for maintaining your privacy and security – for example, by safeguarding your password.

Our Privacy Policy

This is the Privacy Policy of YouScience, LLC ("YouScience," "we," "us," "our") located at 751 Quality Drive, Suite 200, American Fork, UT, 84003. You agree that by accessing our website or signing up for our services (collectively, the "Services"), you allow us to use your Personal Data according to this Privacy Policy. This Privacy Policy applies to all of our products (including aptitude and career discovery and certifications), software, services, mobile applications, and websites as accessed from time to time by you, regardless if the use is in connection with an account or not (collectively, our "Services"). If you have questions or complaints regarding our Privacy Policy or practices, please contact us at privacy@youscience.com or send to the attention of our Privacy Administrator, YouScience, LLC, 751 Quality Drive, Suite 200, American Fork, UT, 84003.

When we use the terms "you," "your," or "user" in this Privacy Policy, we mean to refer to the person who is using our Services and from whom we are collecting information. In some cases, this may include students under the age of thirteen (13) and/or the parents of those students for the purposes of complying with the Children's Online Privacy Protection Act ("COPPA"), as well as the applicable child data protection requirements under the General Data Protection Regulation ("GDPR") for students residing in the European Economic Area ("EEA"). For more information on COPPA, GDPR, and how YouScience complies with data protection regulations, please read the sections titled Child Data Privacy Policies and Your Rights and Choices Regarding Your Personal Data below.

Your Personal Data

In the course of your relationship with us, we collect several types of Personal Data. "Personal Data" is information that can be used to identify you, either alone or in combination with other information. By way of example, we may collect and store the following types of Personal Data:

1. Information that you provide about yourself when registering for and/or purchasing our Services, which may include name, email address, mailing address, user ID, password, and payment

information, except that for children under 13 years of age we do not collect mailing addresses, except for zip codes;

2. Your assessment results, career choices, background information, college choices, educational pathway choices, skills information, interests, job choices, certifications attempted and earned, and other data you provide to or receive from our Services; and
3. All information, data, text, software, music, audio, photographs, graphics, video, messages, or other materials that you provide, except that children under 13 years of age are not permitted to upload any audio, photographs or music and such individuals will not have on-line forum access, though they may communicate directly with customer service through a chat feature.

In some jurisdictions, such as the United States, an IP address may be considered non-personally identifiable data. In the EEA, for example, an IP address is considered Personal Data under applicable data protection laws. If this is the case, we process non-personally identifiable data for the same purposes as Personal Data under this Privacy Policy.

Geolocation Data: You may choose to allow us to access your location by granting the Site access to your location when prompted or through your device's location services settings. You may change these settings on your device.

When you connect to the Services, we are able to recognize the internet (IP) address of the computer providing you with internet access. Our use of this IP address may be to help diagnose problems with our server or otherwise administer our Services. This IP address may also be used to gather broad demographic information. Your IP address is never associated with you as an individual and never provided to another company or organization.

Children's Data: When we collect Personal Data from children under thirteen (13) years old, we take steps to protect children's privacy, including:

- In accordance with applicable law and our practices, requiring that the school administration with whom we have contracted to provide the Services has obtained consent from parents/guardians prior to our collection, use, or disclosure of any Personal Data from children under thirteen (13);
- Limiting our collection of Personal Data from children to no more than is reasonably necessary to participate in an online activity;
- Giving parents/guardians the ability to request access to Personal Data that we have collected from their children and the ability to request that such Personal Data be changed or deleted; and
- Keeping this Privacy Policy updated so that parents, guardians, and schools can read about our information practices regarding children's information, what we collect and how, and whether and with whom we may share that information.

We strongly advise children never to provide any Personal Data in their usernames.

How We May Use Your Personal Data

For Legitimate Interests. We do not sell or rent your Personal Data to any third parties. We may identify you from your Personal Data and merge or co-mingle Personal Data and Non-Personal Data, for any lawful business purpose. Where you provide registration information, cookies can also be used to identify you when you log onto the Services or portions of the Services. Except as otherwise stated, we may use information we collect from you for the legitimate business purpose of providing our Services to you, including, but not limited to:

- to customize the Services to your preferences and to improve your overall experience (e.g., enabling your purchase; providing information, services, products, and user support that you have requested; managing and improving our website, mobile applications, software, and Services; providing customer support; alerting you about new products and services, event information, and career, interests, or education updates; inviting you to participate in specific research projects, conducting quality control; or conducting other research);
- to communicate with you to authenticate your account usage;
- to obtain verified consent from a child's parent or guardian;
- to communicate information and promotional materials to you (where you have not expressed a preference otherwise);
- to identify career, interests, or education information and events pertinent as part of the Services;
- to deliver certification exams
- to check on your account status and maintain record of activities in connection with your use of the Site;
- to notify you of any changes to relevant agreements or policies;
- to enforce our agreements, terms, conditions, and policies;
- to work with our service providers who perform certain business functions or services on our behalf and who are bound by contractual obligations consistent with this Privacy Policy;
- to prevent or investigate fraud (or for risk management purposes), or to comply with legal obligations, court order, or in order to exercise our legal claims or to defend against legal claims;
- to conduct aggregate analysis and develop business intelligence that helps us to enhance, operate, protect, make informed decisions and report on the performances of our Services;
- to describe our Services to current and prospective business partners and to other third parties for other lawful purposes; and
- for other purposes identified to you and as requested by you (please note that you have the right to withdraw your consent to such use at any time by contacting us via the contact information below).

With the Consent of a Data Subject within the EEA; or without consent, if a citizen of any other jurisdiction. If you are a Data Subject within the EEA and we have obtained your consent, we may also use your information in the following ways; and, if you are a citizen of any other jurisdiction, you acknowledge that we may use your information in the following ways:

- to share your information with our corporate parents, subsidiaries, other affiliated entities, and associated entities for the purposes described in this Privacy Policy;
- to send e-mail and postal mail to provide you with updates and news;
- to process any request, you make;
- to process any commercial transaction, including, but not limited to, fulfilling an order or subscription request; and
- to process your Personal Data as described throughout this Privacy Policy.

Performance of a Contract. If you have agreed to our terms of use, or other terms of service, and you have created an account, purchased merchandise, signed up for a subscription, or entered into a contest or sweepstakes, we may also use your information:

- to establish your account to use the Services and validate your username, e-mail, password, and/or other login credentials
- to respond to your requests
- to provide you with merchandise you have requested
- to fulfill your subscription purchase(s)
- to notify you of your contest or sweepstakes results
- to send you e-mail and postal mail supplying you with the most recent service information or to send you information about your order (e.g., order confirmations, shipment notifications, etc.)
- to notify you of any changes to relevant agreements or policies
- to process your Non-Personal Data as outlined as described throughout this Policy

We may use third-party e-mail providers to deliver these communications to you. This is an opt-in e-mail program. If you no longer want to receive these e-mail communications, you may opt-out of receiving email communications.

We may, from time to time, invite you to participate in online surveys. The information requested in these surveys may include, but is not limited to, your opinions, beliefs, insights, ideas, activities, experience, purchase history, and purchase intent regarding products, events, and Services. The information collected by these surveys is used to research market trends, company growth, community needs, etc. Your input will help us to improve customer experience and shape development of our products and Services.

How We May Share Your Personal Data

If someone, including a parent or institutional purchaser, has purchased the Services for you and you accept the Service, we share status updates with them to indicate your progress, and make data available to them, including your assessment results, career choices, background information, college choices, educational

pathway choices, skills information, interests, job choices, and other data you provide to or receive from our Services.

We do not release your identifiable Personal Data to anyone other than as directed by you and the purchaser of the Services without asking for and receiving explicit consent to do so from you (or a parent/guardian if the Personal Data pertains to a child under thirteen (13) years old), unless necessary to provide you our Services (e.g. credit card processing) or as required by law.

If you choose to complete a transaction on or through features on the Services using a credit or debit card, we may forward your information to third parties for services such as credit card or other payment processing. We utilize Stripe to process such payment transactions. To complete such payments, you will be required to provide Personal Data, together with your payment information (including but not limited to, your credit card number). For such transactions, YouScience will only receive the transaction record (name, payment amount, date, time, etc.). YouScience does not collect or store your payment information, including credit card number; rather, Stripe collects and stores the payment information you enter. To learn more about Stripe's policies, you can visit its website [here](#).

We give you the ability to share your identifiable Personal Data with your collaborators (e.g. parents, counselors, and others), prospective employers, friends, and others through sharing features; however, this is entirely controlled by you and optional within the Services.

Only if you explicitly consent, we may share your Personal Data with third parties for the purpose of informing you about educational opportunities, careers, or other non-YouScience services that may be relevant to you.

Personal Data You Share Through The Services

- We may give you the ability to connect with other individuals to share information. In addition, you may choose to disclose your own information through other means, such as a printable PDF report, including any part of your Personal Data to friends and/or family members, counselors, groups of individuals, third-party service providers, employers, educators, and/or other individuals. We recommend that you make such choices carefully.
- Your posts to community forums are publicly displayed, and you grant us a non-exclusive license to publicly use and display any material you post. We may make such posted material available to other companies, organizations, or individuals with whom we have relationships, and use such material in connection with the provision of our Services, except that we reserve the right to discontinue access to any or all community forums at any time and users under thirteen (13) years old may be denied such access entirely.
- Additionally, if you choose to access, visit, and/or use any third-party social networking service(s) that may be integrated with our Services, we may receive your Personal Data and other information about you and your computer, mobile, or other device that you have made available to those social networking services, including information about your contacts on those services. For example, some social networking services allow you to push content from our Service to your contacts or to pull information about your contacts so you can connect with them on or through our Service. Some

social networking services also will facilitate your registration for our Service or enhance or personalize your experience on our Service. Your decision to use a social networking service in connection with our Service is voluntary. However, you should make sure you are comfortable with the information your third-party social networking services may make available to our Service by visiting those services' privacy policies and/or modifying your privacy settings directly with those services.

- Personal Data, once released or shared, can be difficult to contain. We have no responsibility or liability for any consequences that may result because you release or share your Personal Data with a third party beyond our control. It is incumbent upon you to share Personal Data only with people you know and trust.
- If you have a multi-profile account, you should use caution in setting profile-level privacy settings. If you provide us information about others for the purposes of sharing your Personal Data, we will use the information you provide to contact such person on your behalf as part of the Services. You agree that under no circumstances will you provide us information about any individual who is under thirteen (13) years old.
- You must opt-out of some features to avoid notifications. We give you the opportunity to opt out of optional communications, either through our Service or by contacting our Privacy Administrator at privacy@youscience.com. Likewise, if you are reading this because you have access to the Personal Data of a YouScience customer through a multi-profile account, we urge you to recognize your responsibility to protect the privacy of that customer, and you agree to use that Personal Data only for the purpose it is being shared with you.

Third-Party Service Providers

Service providers help us administer and provide the Services (for example, a web hosting company whose services we use to host our platform). These third-party services providers have access to your Personal Data only for the purpose of performing services on our behalf. We require these service providers to comply with all applicable data privacy laws and regulations and to use Personal Data only for the purposes for which it was disclosed. We require that any third-party service providers limit their use of your information solely to providing services to us and that they maintain the confidentiality, security, and integrity of your Data and not make unauthorized use or disclosure of the Data. Our third-party service providers are as follows:

- Amazon Web Services, a subsidiary of Amazon- system hosting
- Heroku, a subsidiary of Salesforce.com- system hosting and monitoring
- Google- system hosting and analytics

We use commercially reasonable efforts to engage with third parties that post a privacy policy governing their collection, processing, and use of Personal Data. While we may seek to require such third parties to follow appropriate privacy policies and will not authorize them to use this information except for the

express purpose for which it is provided, and you agree that we do not bear any responsibility for any actions or policies of third parties.

Children's Data Privacy Policies

YouScience is committed to protecting the privacy of children who use our Services. As the parent or guardian of a child under the age of thirteen (13), who has been signed up to use our Services, you have certain rights pursuant to COPPA regarding the collection, use, and/or disclosure of your child's Personal Data:

- You may review the Personal Data submitted by your child through our Services at any time by contacting our Privacy Administrator at privacy@youscience.com. You may be required to provide verifiable confirmation of your identity in relation to the child whose data you seek to review.
- By contacting our Privacy Administrator at privacy@youscience.com, you may direct us to delete your child's Personal Data that YouScience has collected through the Services or withdraw your consent to any further collection or use of the Personal Data.
- You always have the option of consenting to the collection and use of your child's Personal Data through our Services, but not to our sharing of the Personal Data with any third parties.

Unless you have alerted us to your preference otherwise regarding your child's information, we may share or disclose Personal Data collected from children in a limited number of instances, including the following:

- We may share Personal Data with our service providers only as necessary for them to perform a business, professional, or technology support function for us.
- We may disclose Personal Data to the school administrators with whom we have contracted to provide the Services to the students.
- We may disclose Personal Data if required by law, for example, in response to a court order or a subpoena. To the extent permitted by applicable law, we also may disclose personal information collected from children (i) in response to a law enforcement or public agency's (including schools or children services) request; (ii) if we believe disclosure may prevent the instigation of a crime, facilitate an investigation related to public safety or protect the safety of a child using our sites or applications; (iii) to protect the security or integrity of our sites, applications, and other technology, as well as the technology of our service providers; or (iv) enable us to take precautions against liability.

As with all of our users of any age, we will never require a child to disclose more Personal Data than is reasonably necessary to participate in our Services and we do not retain any Personal Data for any user longer than is required to fulfill the purposes for which the Personal Data was supplied to us.

In certain circumstances, school administrators are permitted to act in the stead of parents and guardians for purposes of granting consent to the collection of Personal Data from children when we have contracted with

the school to provide our Services. We contractually require that all of our school administration partners obtain verifiable parental consent from the parents and guardians of students under thirteen (13) years old prior to our providing our Services or collecting any Personal Data. As a matter of best practice, we also highly recommend that our school administration partners provide parents and guardians with notices of our policies and online services, as well as any direct notices that we provide to the school to fulfill our COPPA compliance requirements. Within the scope of the consent we have obtained from the school administrators, we will treat the Personal Data of children only in accordance with our instruction received from the school. This in no way limits your rights as a parent or guardian to review, request deletion of, or limit our usage of your child's Personal Data, as described above.

On occasion, in order to respond to a question or request from a child, YouScience may need to ask for the child's online contact information, such as an email address. We will delete this information immediately after responding to the question or request.

Whenever we collect a child's online contact information for ongoing communications, such as to provide a newsletter with occasional updates about our website and/or Services, we will simultaneously require a parent/guardian email address in order to notify the parent/guardian about the collection and use of the child's information, as well as to provide an opportunity to object to our further contacting the child.

For more information about COPPA and general tips about protecting children's online privacy, please visit the FTC's website [here](#).

How We Use Web Behavior Information

"Web Behavior Information" is information on how you use our Services (e.g. browser type, domains, page views) collected through log files, cookies, and web beacon technology during your visits to the YouScience website. We use Web Behavior Information to improve our Services and your overall experience and to track and monitor aggregate usage of our website and/or to target advertising for our products and services. We may also use your Web Behavior Information the same as other non-Personal Data (described below), so long as it is de-identified.

- **Log Files.** When you visit our website or use our mobile application, we gather certain information automatically and store it in log files. This information includes your Internet Protocol (IP) addresses, browser type, Internet Service Provider, referring/exit pages, operating system, date/time stamp, and clickstream data (i.e. a list of pages or URLs visited). We may link this information to your profile ID or account. We use this information to analyze trends, administer the site, track movements around the site, identify and resolve issues, and gather demographic information about our user base as a whole.
- **Cookies.** Our website uses cookies. Cookies are pieces of information that a website transfers to your browser for record-keeping purposes about your use of a website. These cookies will be placed as a text file in your browser.
- **Web Beacons.** A web beacon is a clear graphic image that is loaded by your web browser when it accesses a website and that records your visit to a particular web page. We, or third parties that work for us, may place cookies and web beacons on our website, in emails, and in advertisements on other websites. The purpose of our web beacons is to support our Services and

to promote our products and services through targeted advertisements. If you wish to disable web beacons, you may configure your browser to prevent loading them.

When children use our Services, we may also collect Web Behavior Information automatically. In the event that we collect (or allow others to collect) such information from children on Services for purposes other than those described above, we will notify parents/guardians and obtain verifiable parental consent prior to such collection.

We May Use De-Identified Information

We may use data and information about you that has been "de-identified" (data from which your name or any personally identifying information has been removed, or the data has been combined with other people's data in such a way that it is no longer associated with you) for any purpose — it is no longer Personal Data.

Security

We take security seriously. We use a range of reasonable physical, technical, and administrative measures to safeguard your Personal Data, in accordance with current technological and industry standards. In particular, all connections to and from our website and mobile application are encrypted using Secure Socket Layer (SSL) technology. Protecting your Personal Data is also your responsibility. You are responsible for safeguarding your password, secret questions and answers, and other authentication information you use to access our Services. You should not disclose your authentication information to any third party, and you should immediately notify us of any unauthorized use of your password. We cannot secure Personal Data that you release or that you request us to release.

Your Rights and Choices Regarding Your Personal Data

You may change, edit, update, or delete the information that you provided when you set up your account through our Service(s) through your account settings. If you no longer wish to receive our Services, you may close your account by sending a written request to support@youscience.com. When closing an account, we remove all Personal Data from your account (or profile) within thirty (30) days of our receipt of your request. We may continue to use de-identified Personal Data after you close your account for any lawful purpose.

If you reside in certain jurisdictions, such as the EEA, you may have additional rights and options with regard to accessing, reviewing, correcting, and updating your Personal Data, as well as how we use and disclose your Personal Data. As a Data Subject under GDPR, you have the right to request access to your Personal Data as it exists in our records by contacting our Privacy Administrator at privacy@youscience.com. You also have the right to rectification, correction, or amendment of your Personal Data if it is inaccurate or incomplete. You may also have the right to erasure of your Personal Data; however, this is not always possible due to legal requirements and exceptions may apply.

A Data Subject may have the right to object to the processing of his or her Personal Data, for example, due to his or her particular situation, for direct marketing uses, or for scientific or historical research. In certain circumstances, Data Subjects may have the right to obtain a restriction on our processing of their Personal Data, in which case such Personal Data will, with the exception of storage, only be processed with the Data Subject's consent or in circumstances such as our exercise or defense of legal claims or the protection of another person. Data Subjects may also have the right to request that we provide data portability for their Personal Data via a copy of the data in a commonly-used format and/or transfer their Personal Data directly to another data controller (where technically feasible). Exceptions to these rights may apply, for example, if the processing is necessary for a task carried out in the public interest. Finally, if a Data Subject has given his or her consent to our processing of his or her Personal Data for certain purposes, he or she has the right to withdraw consent to such use at any time by contacting us via the contact information below:

You can also opt-out of receiving certain messages or notifications by contacting our Privacy Administrator at privacy@youscience.com. You can also click the "unsubscribe" button at the bottom of promotional email communications. Please note that you may not opt-out of receiving non-promotional messages regarding your account, such as technical notices, purchase confirmations, or Service-related emails. You can configure your browser to enable, disable or delete cookies. Please note that if you set your browser to disable cookies, you may not be able to access secure areas of the website and other parts of the website may also not work properly.

You may also choose to stop or start receiving our newsletter or marketing emails by contacting us at marketing@youscience.com.

Data Protection Officer

Our appointed Data Protection Officer is Brett McCleary. If you have an inquiry regarding your Personal Data, pursuant to the rights listed in the preceding section (above), please send your message to the following email: privacy@youscience.com. You may also contact him at (801) 653-9356.

Geographic Data Transfers

We take steps to ensure that transfers of Personal Data are performed in accordance with applicable law and carefully managed to protect your privacy rights and interests. If you are a Data Subject, in some instances we may need to transfer your Personal Data outside the EEA. Transfers are limited to countries that are recognized as providing an adequate level of legal protection or where we can be satisfied that alternative arrangements are in place to protect your privacy rights. Therefore, where we transfer your Personal Data outside our corporate affiliates or to third parties who help provide our products and services, we obtain contractual commitments to protect your Personal Data under Data Protection Agreements and pursuant to standard contractual clauses. Some of these assurances are well recognized certification schemes, such as the EU—US Privacy Shield for the protection of Personal Data transferred from within the European Union to the United States. Where we receive requests for information from law enforcement or regulators, we carefully validate these requests before disclosing any Personal Data.

Information Disclosure Required By Law

Under certain circumstances Personal Data may be subject to disclosure pursuant to judicial or other government subpoenas, warrants, or orders, or in coordination with regulatory authorities. You acknowledge and agree that YouScience is free to preserve and disclose any and all Personal Data to law enforcement agencies or others if required to do so by law or in the good faith belief that such preservation or disclosure is reasonably necessary.

Linked Websites

We provide links to third-party websites operated by organizations that are not affiliated with YouScience. We do not disclose your Personal Data to these organizations. We do not review or endorse, and we are not responsible for, the privacy practices of these organizations. We encourage you to read their privacy statements. This Privacy Policy applies solely to information collected by YouScience.

Your California Privacy Rights

California Civil Code Section 1798.83 permits California residents to request and obtain a list of what Personal Data (if any) we disclosed to third parties for direct marketing purposes in the preceding calendar year and the names and addresses of those third parties. Requests may be made only once a year and are free of charge. Under Section 1798.83, California residents are entitled to request and obtain such information, by e-mailing a request to privacy@youscience.com.

Business Transitions

In the event that we go through a business transition such as a merger, acquisition by another company, or sale of all or a portion of its assets, your Personal Data will likely be among the assets transferred. In such a case, your information would remain subject to our Privacy Policy.

Changes to This Privacy Policy

We reserve the right to modify and update this Privacy Policy at any time by posting an amended version of the statement on our Site. Please refer to this policy regularly. If at any time we decide to use Personal Data in a manner different from that stated at the time it was collected, we will notify you either on the panel home page of our Site or via e-mail.

How to Contact Us

Because protecting your privacy is important to us, you may always submit concerns regarding our Privacy Policy on the contact us page. We will attempt to respond to all reasonable concerns and inquiries expeditiously. If you have any questions or comments about our Privacy Policy, please contact us at: support@youscience.com or (801) 653-9356.