SAVVAS
LEARNING COMPANY

Data Processing Agreement

If you are subject to the European Union Data Protection Directive 95/46/EC, General Data Protection Regulation (2016/EC/679) or "GDPR"), or similar statute ("Data Protection Laws"), the terms of this Data Processing Agreement (the "Agreement") shall govern the processing of Customer Data (as defined below) provided by your educational institution (referred to herein as the "Data Controller," "Customer," "you," and "your") to Savvas Learning Company LLC (referred to herein as the "Data Processor," "Savvas," "we," "us," and "our") for the purposes of facilitating the use by you and your students, teachers, administrators or other users ("Authorized End Users") of Savvas' digitally-delivered educational solutions (the "Services"). Customer and Savvas may each be referred to herein as a "Party" or collectively as the "Parties."

The following provisions shall apply whenever Customer Data is processed on your behalf:

1. Savvas' obligations

1.1 We shall process personal data and information provided by you or your Authorized End Users ("**Customer Data**") within the scope of this Agreement, for the purpose of the provision of the Services during the term of your subscription to the Services, and pursuant to your documented instructions (unless required to process Customer Data other than instructed by applicable law, in which case we will, before processing Customer Data in accordance with that law, inform you unless that law prohibits us from doing so). You warrant your collection and sharing of Customer Data with us and our processing of Customer Data in accordance with your instructions shall comply with applicable law. We shall not compile copies or duplicates without your approval, except for copies made for backup or disaster recovery purposes.

1.2 Annex A of this Agreement contains a list of the categories of Customer Data, the data subjects concerned, and the nature and purpose of processing Customer Data.

2. Authority to issue instructions

2.1 We agree, without limitation, to strictly follow any instructions given by you under this Agreement as well as those issued on an individual basis with regard to the collection, processing and/or usage of Customer Data. This includes but is not limited to instructions on the blocking, correction or deletion of Customer Data. Our obligations under this Section 2.1 shall be subject to Section 2.3.

2.2 Instructions may only be issued by your management board, data protection officers or the manager of your legal department, if applicable (hereinafter "**persons authorized to issue instructions**"). The persons authorized to issue instructions shall have the right, at all times, to make written appointments of additional persons authorized to issue instructions.

2.3 You warrant that you shall give only lawful instructions. If we hold the view that any instruction of yours contravenes statutory regulations and/or the Agreement, we will notify you, and we are entitled to suspend execution of the instruction concerned, until you confirm such instruction in writing. We have the right to deny the execution of an instruction – even if issued in writing – in case we conclude that we would be liable under applicable law if we execute the instructions you have provided.

2.4 We shall, by way of regular self-audits, ensure that the processing of Customer Data on your behalf conforms to this Agreement.

3. Data secrecy

3.1 We undertake to maintain data secrecy, pursuant to applicable Data Protection Laws, and keep Customer Data confidential. In particular, we will ensure that such persons with access to Customer Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.We confirm that we are aware of the applicable Data Protection Laws. We agree that we make our applicable employees familiar with the relevant provisions of data protection regulations. We shall supervise compliance of such employees with applicable Data Protection Laws.

3.2 We confirm that we are aware of the applicable Data Protection Laws. We agree that we make our applicable employees familiar with the relevant provisions of data protection regulations. We shall supervise compliance of such employees with applicable Data Protection Laws.

4. Subprocessing

4.1 Subprocessing for the purpose of this Agreement is to be understood as meaning processing which relates directly to the Services provided to you. This does not include ancillary services commissioned by us, such as telecommunication services, postal / transport services, cleaning or guarding services. IT services shall constitute a Subprocessing relationship if they are provided for IT systems which are used for the delivery of the Services you have purchased from us. We shall, however, be obliged to make appropriate and legally binding contractual arrangements including technical and organizational measures and take appropriate inspection measures to ensure the data protection and the data security of your data, even in the case of outsourced ancillary services.

4.2 In accordance with the provisions of this Agreement, you acknowledge and agree that Savvas, or the third parties engaged to provide the Services provided here: https://assets.savvas.com/asset_mgr/current/202114/Subprocessor%20List_LOr3.pdf
(which are hereby designated as subprocessors for the purpose of processing Customer Data) may store or process Customer Data in locations outside the country in which you are located on servers based in the United States provided that (a) we shall publish notification of any changes to the subprocessors processing Customer Data on our website thirty (30) days prior to any changes to the subprocessors processing Customer Data and give you an opportunity to review such changes and raise reasonable objection to such changes; and (b) the subprocessors processing Customer Data are subject to the same data protection obligations or the same level of protection as are contained in this Agreement in accordance with Article 28 paragraphs 2-4 GDPR. Customer agrees to raise any reasonable objections in writing within ten (10) calendar days of such notification. In the event you reasonably object to the addition of a Subprocessor for reasons related to the GDPR, as permitted in the preceding sentences, and the Parties do not find a solution in good faith to the issue in question, then either Party may terminate this Agreement and we will provide a pro-rated refund for any prepaid but unused fees. You confirm that Section 4.2 constitutes general written authorization for the purposes of GDPR. We shall remain liable for any processing of Customer Data carried out by subprocessors engaged under the Agreement. Upon your request, we will tell you where Customer Data is located. Notwithstanding anything to the contrary in this Section, if we and you have agreed that Customer Data will be stored in any particular location, we will store such Customer Data in the agreed location.

SAVVAS
LEARNING COMPANY

5. International Data Transfers

5.1 We recognize any transfer of Customer Data to an organization outside the European Economic Area ("EEA") or to any country which has not been the subject of a European Commission adequacy decision requires documented instructions from you and compliance with the requirements for the transfer of personal data to third countries pursuant to Chapter V of the GDPR. To the maximum extent permitted by law, Customer agrees and allows Customer Data to be transferred to, and hosted on, servers based in the United States. Section 7 specifies the Data Security measures to ensure an adequate level of data protection under Article 44 et seq. GDPR within the framework of this Agreement.

6. Audit

6.1 Upon request, we will provide you an overview of our data processing operations, to include the following information:

(a) owners, managing boards, managing directors or other lawfully or constitutionally appointed managers and the persons placed in charge of the Customer Data processing;

(b) our address;

(c) purposes of collecting, processing or using the Customer Data;

(d) a description of the groups of data subjects and the Customer Data or categories of Customer Data;

(e) recipients or categories of recipients to whom the Customer Data may be transferred;

(f) standard periods for the retention of Customer Data;

(g) any planned data transfer to other countries; and

(h) a general description enabling a preliminary assessment as to whether the technical and organizational measures to guarantee the safety of processing are adequate.

The Parties agree and acknowledge that for the purposes of this Section 6.1 it shall be sufficient that we present all documentation, including a certified statement on the compliance with this Agreement, in such format as reasonably required by you or any independent auditor appointed by you at your expense. We shall make available to you any other information you request where necessary to demonstrate compliance with your obligations under Article 28 of the GDPR unless in our opinion such a request infringes Data Protection Laws or European Union or Member State law, in which case we shall inform you of our opinion.

6.2 You have the right to audit our compliance with the statutory regulations on data protection and the stipulations entered into between the Parties (including the technical and organizational measures), by requesting information about and inspecting storage of the Customer Data, and implemented policies and security incident reports, subject to reasonable prior notice of at least 14 days in advance and, to the extent reasonably possible, without interfering with our regular business operations on a date and at a location determined by us. Notwithstanding the foregoing, if our organization has completed a third-party audit of its security practices and procedures within the preceding twelve (12) months, we may supply you with a copy of a summary of the results of such audit in lieu of conducting an audit itself.

6.3 Customer agrees that, taking into account the nature of the processing of Customer Data under this Agreement, by providing the assistance and information contained in this Agreement, we have assisted you in ensuring compliance with your obligations in respect of data protection impact assessments and prior consultation under Articles 35 and 36 of the GDPR.

7. Data security measures

7.1 We use the following appropriate technical and organizational measures to protect Customer Data ("Security Measures"), which must meet, at a minimum, the level required by applicable law:

(a) Admission control:

- We employ appropriate physical safeguards to prevent unauthorized persons from gaining access to the premises where Customer Data is collected, processed and used. Such premises may only be entered by us and/or our agents.
- We use appropriate measures to secure buildings.
- We use appropriate measures to ensure that Customer Data held in hardcopy are kept securely, e.g., in locked rooms or filing cabinets. Generally, steps are taken to ensure that access to hardcopy Customer Data is limited in the same way it would be on an electronic IT system, i.e., access is limited to those individuals where it is necessary for them to have access in order for them to perform their job role.

(b) Entry control:

- We shall endeavor to prevent unauthorized parties from accessing or using our data processing systems.
- We shall require authentication and authorization to gain access to IT systems (i.e., require users to enter a user id and password before they are permitted access to IT systems).
- We have procedures in place to permit only authorized persons to access Customer Data internally or externally by using authentication procedures (e.g., by means of appropriate passwords), except as otherwise enabled by you.

(c) Access control:

- We employ appropriate measures to prevent individuals accessing Customer Data unless they hold a specific access authorization.
- We employ appropriate measures to only permit user access to Customer Data which the user needs to access for his/her job role or the purpose access to our IT systems is provided (i.e., we implement measures to ensure least privilege access to IT systems).
- We have in place appropriate procedures for controlling the allocation and revocation of Customer Data access rights such as, for example, appropriate offboarding procedures for revoking employee access to IT systems upon job or role change.

- Our systems that are used to collect, process and use Customer Data are protected by user identifiers, passwords and graded access rights. Special access rights are provided for the purposes of technical maintenance and do not allow access to Customer Data.

- We take appropriate administrative safeguards to protect our services against external attacks, including, for example, deploying firewalls.

(d) Transmission control:

- We employ appropriate measures to protect the confidentiality, integrity and availability of Customer Data during electronic transmission.

- We encrypt the Customer Data items listed in Annex A while in transit over the internet.

(e) Input control:

- We maintain logging and auditing systems to monitor activity related to the input of Customer Data.

(f) Order control:

- We ensure that all requests from you with respect to Customer Data are processed strictly in compliance with your instructions through the use of clear and unambiguous contract terms and/or monitoring of contract performance.

(g) Availability control:

- We protect Customer Data in our possession against unintentional destruction or loss by implementing appropriate management, operations, and technical controls such as firewalls; monitoring; and back-up procedures.

- Example measures that may also be taken include: mirroring of storage media, uninterruptible power supply (UPS); remote storage; firewall systems; and disaster recovery plans.

7.2 The technical and organizational measures described in Section 7.1 are subject to technological advancements and further development. We are permitted to implement suitable alternative measures, as long as the alternative measures do not reduce the level of security applied to the Customer Data.

7.3 We regularly audit and assess our compliance with the technical and organizational security measures.

8. Notification duties

SAVVAS
LEARNING COMPANY

8.1 Notification of infringements of data protection regulations

(a) We shall notify you to the extent the technical and organizational measures taken by us are not in accordance with this Agreement or your instructions. The same applies to malfunctions or indications for an infringement of data protection regulations, or in case of improper processing of Customer Data, including, but not limited to, data security breaches and data losses. We and you shall mutually agree on any further collection, processing and usage of Customer Data, and we shall initiate all reasonably necessary measures to exclude risks to the integrity and confidentiality of Customer Data.

(b) In the event we have a reasonable, verifiable belief that an unauthorized third party has gained access to or disclosed your Customer Data, we will promptly, or if required by Law in such other time required by such Law, notify you. We will provide you with reasonable cooperation and assistance in relation to your investigation of the incident. If such incident triggers any third-party notice requirements under Laws, you agree that unless otherwise required by Law, as the owner of the Customer Data, you will be responsible for the timing, content, cost and method of any such notice and compliance with such Laws.

8.2 You agree that, given the nature of the processing, Section 8.1 satisfies our obligation to assist you with your obligations under Articles 33 and 34 of the GDPR.

8.3 We shall notify you about:

(a) any legally binding request for disclosure of the Customer Data by a law enforcement authority or other organization or body, unless prohibited by law;

(b) any request received directly by us from a data subject.

8.4 We agree to provide you with reasonable cooperation and assistance in relation to any request under Section 8.3. You agree that, given the nature of the processing, Section 8.3 satisfies our obligation to assist you by appropriate technical and organizational measures, insofar as this is possible, for fulfillment of Customer's obligations to respond to requests for exercising rights laid down in Chapter III of the GDPR.

9. Deletion of data

9.1 Upon expiration or earlier termination of the processing services, or such earlier time as you request, we agree, at your written request, to securely destroy or render unreadable or undecipherable, the relevant Customer Data in our possession, custody or control.

9.2 We shall ensure from an organizational perspective that Customer Data can be deleted within a reasonable time frame consistent with your request or deletion requirements established in the Agreement, except that we shall not be obliged to delete Customer Data from archival and back- up files unless such deletion is in line with our company data retention schedule (as permitted under Data Protection Legislation). If you request deletion of Customer Data in archival and back-up-files, you shall bear the costs including costs for business interruptions associated with such request.

SAVVAS
LEARNING COMPANY

10. Final Provisions

10.1 Unless specifically stipulated to the contrary by the Parties, the duration of the commissioned data processing specified by this Agreement shall be coterminous with the length of Customer's subscription to the Services.

10.2 We may update our Terms of Use and/or Privacy Policy from time to time to better reflect changes to the law, new regulatory requirements or improvement to the Services. The updated Terms of Use shall be posted here: https://www.savvasrealize.com/userAgreement.html and updates to our Privacy Policy shall be posted here: https://www.savvasrealize.com/privacy/corporate/privacy/learning-services-privacy-policy.html. If any update(s) materially affect the terms of this Agreement or your use of the Services or your rights herein, we will provide 30 days' prior notice at the link(s) above or in-product notification. Your continued use of the Services shall constitute acceptance to be bound by the updated terms.

10.3 In the event of a conflict between this Agreement and any other provision of the Terms of Use, our Privacy Policy, or any other agreement between you and us, this Agreement will prevail.

On behalf of the Data Processor: **Savvas Learning Company LLC**

Name (written out in full):	Kevin Schutz
Position:	VP & Senior Counsel
Address:	15 E Midland Ave Ste 502 Paramus, NJ, 07652-2938 United States
Signature	

On behalf of the Data Controller: _____

Name (written out in full):	
Position:	
Address:	
Signature	

SAVVAS
LEARNING COMPANY

Annex A – Details of the Data Processing

Categories of Data

Student name or unique identifier
Personal contact information, including email
Grade Level, School ID Number, Teachers, Classes/Sections/Courses, Grades, Assignments, Tests, Books, Attendance, Homework, Program Performance
Usernames, passwords
IP Addresses of users, User or Customer Correspondence, Meta data on user interaction with application
Observation and assessment data
Personal information contained in content generated and/or provided by an Authorized User such as submitted papers, assignments, blog and discussion posts, contributions to online collaboration

Special Categories of Data (if any)

Savvas' Services are generally not intended to Process Special Categories of Personal Information. Any Processing of Special Categories of Personal Information is determined and controlled by you in compliance with Applicable Data Privacy Laws.

Categories of Data Subject:

Customer and Customer's Authorized End Users (Students, Teachers and Administrators)

Nature of Processing:

We shall process data and information provided by you or your Authorized End Users within the scope of the Agreement, for the delivery of our Services during the term of your subscription to the Services, and pursuant to your documented instructions (unless required to process Customer Data other than instructed by applicable law, in which case we will, before processing Customer Personal Data in accordance with that law, inform you unless that law prohibits us from doing so).