STANDARD STUDENT DATA PRIVACY AGREEMENT

MO-NDPA Standard
Version 1.0

Rockwood R-VI School District

and

Savvas Learning Company LLC

7. **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 LEA for this DPA is:

Name: Deborah Ketring

Title: Chief Information Officer (CIO)

Address:
111 E. North St., Eureka, Missouri 63025

Phone: (636)733-1103

Email: ketringdeborah@rsdmo.org

The designated representative for the Provider for this DPA is:

Name: Jeff Burklo Title: Director, Data Privacy and Security

Address: 15 E. Midland Ave., Suite 502, Paramus, NJ 07652

Phone: (201) 928-7770

Email: Jeff.Burklo@Savvas.com

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

LEA

Rockwood R-VI School District

By: Deborah Ketring Date: 7/7/2021

Printed Name: Deborah Ketring Title/Position: CIO

Savvas Learning Company LLC

By: Kevin Schutz Kevin Schutz (Jul 7, 2021 11:06 PDT) Date: 07/07/2021

Printed Name: Kevin Schutz Title/Position: VP & Senior Counsel

ACKNOWLEDGED AND AGREED with respect to products owned by Pearson Education, Inc.:

By: Robert Klein Robert Klein (Jul 7, 2021 14:00 EDT) Printed Name: Robert Klein

Title: Finance Director Date: 07/07/2021

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.

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-

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. Notwithstanding the foregoing, if Provider has completed a third-party audit of its security practices and procedures within the preceding twelve (12) months, Provider may supply LEA with a copy of a summary of the results of such audit in lieu of LEA conducting an audit itself.

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 five (5) business days 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

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 "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.	Realize myLab and Mastering
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	Realize myLab and Mastering
Assessment	Standardized test scores	
	Observation data	
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications captured (emails, blog entries)	
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, or primary language spoken by student)	
	Other demographic information-Please specify:	
Enrollment	Student school enrollment	Realize myLab and Mastering
	Student grade level	Realize myLab and Mastering
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information-Please specify:	
Parent/Guardian	Address	

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

EXHIBIT "C"
DEFINITIONS

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.

EXHIBIT "D"
DIRECTIVE FOR DISPOSITION OF DATA

Rockwood R-VI School District Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. The terms of the Disposition are set forth below:

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:

Insert categories of data here

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

2. Nature of Disposition

x ____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:

Insert or attach Special Instructions

3. Schedule of Disposition

Data shall be disposed of by the following date:

x ____As soon as commercially practicable.

_____ By Insert Date Here

4. Signature

Deborah Kitsmiller
Authorized Representative of LEA

7/7/2021
Date

5. Verification of Disposition of Data

_____
Authorized Representative of Company

_____
Date

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

	MAINTAINING ORGANIZATION/GROUP	FRAMEWORK(S)
X	National Institute of Standards and Technology	NIST Cybersecurity Framework Version 1.1
X	National Institute of Standards and Technology	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
	International Standards Organization	Information technology — Security techniques — Information security management systems (ISO 27000 series)
	Secure Controls Framework Council, LLC	Security Controls Framework (SCF)
	Center for Internet Security	CIS Critical Security Controls (CSC, CIS Top 20)
	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

EXHIBIT "H"

Additional Terms or Modifications

Version 1.0

As used in this Exhibit H, the term "Agreement" shall refer to the DPA and the Service Agreement collectively. LEA and Provider agree to the following additional terms and modifications to the DPA:

1. Article IV, Section 3 of the DPA, Provider Employee Obligation, is hereby supplemented by adding three new sentences to the end of the Section to read as follows:

   Provider shall require that its employees, contractors, and agents who have access to Student Data pursuant to the DPA complete periodic security training. Provider shall keep true and complete records of any and all Student Data received, exchanged and shared between and amongst its employees, agents, and contractors and permit LEA to access such records upon request. Provider shall also outline for LEA upon request the steps and processes that Provider will take to prevent post-employment data breaches by Provider employees after their employment with Provider has been terminated.

2. Article IV, Section 4 of the DPA, No Disclosure, is hereby supplemented by adding one new sentence to the beginning of the Section to read as follows:

   Provider shall exclusively limit its employees, contractors, and agents' access to and use of Student Data to those individuals who have a legitimate need to access Student Data in order to provide services to the LEA.

3. The second sentence of Article IV, Section 7 of the DPA, Advertising Limitations, is hereby deleted in its entirety and one new sentence is inserted to read as follows:

   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) from otherwise using Student Data as permitted in this DPA and its accompanying exhibits.

4. The first sentence of Article V, Section 1 of the DPA, Data Storage, is hereby deleted in its entirety and replaced with one new sentence to read as follows:

   Student Data shall be stored within the United States.

5. Article V, Section 3 of the DPA, Data Security, shall be supplemented by adding three new sentences to the end of the Section to read as follows:

   In conducting data transactions and transfers with the LEA, Provider shall ensure that all such transactions and transfers are encrypted. Provider represents and warrants that all of its data portals are secured through the use of verified digital certificates. Upon request, Provider shall provide LEA with a data inventory that inventories all data fields and delineates which fields are encrypted within Provider's platform maintaining collected Student Data.

6. Article V, Section 4 of the DPA, Data Breach, is hereby modified as follows:

   a. The first sentence of Section 4 shall be deleted in its entirety and one new sentence is inserted to read as follows:

      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 five (5) business days of confirmation of the incident,

12. **Indemnity.** Provider agrees to indemnify, defend, and hold harmless the LEA, its Board of Education, officers, directors, employees, representatives, agents, successors, and assigns from, against, and in respect to any and all claims, losses, damages, suits, or liabilities, including costs and attorneys' fees, for damages incurred or suffered, directly or indirectly, to the extent arising from or relating to the acts and/or omissions of Provider and/or its employees, contractors, or agents, in connection with providing the services, as is contemplated under this Agreement.
13. **Insurance**. At all times during the term of the Agreement, Provider shall maintain, at its sole cost and expense, insurance coverage as follows: (i) Commercial General Liability insurance in an amount not less than $1,000,000 per occurrence and $2,000,000 in aggregate; and (ii) Cyber Security insurance in an amount not less than $1,000,000 per occurrence and $2,000,000 in aggregate. LEA shall be named as an additional insured on the commercial general liability policy and all such insurance coverage shall be primary and non-contributory with respect to any insurance maintained by LEA. Copies of Provider's certificates of insurance showing the required coverage shall be provided to LEA upon execution.
14. **Force Majeure.** If either party is prevented from performing any of its obligations due to any cause which is beyond the non-performing party's reasonable control, including fire, explosion, flood, epidemic/pandemic or other acts of God; acts, regulations, or laws of any government; strike, lock-out or labor disturbances; or failure of public utilities or common carriers (a "Force Majeure Event"), such non-performing party shall not be liable for breach of this Agreement with respect to such non-performance to the extent any such non-performance is due to a Force Majeure Event. Such non-performance will be excused for three months or as long as such event shall be continuing (whichever occurs sooner), provided that the non-performing party gives immediate written notice to the other party of the Force Majeure Event.
15. **Disputes.** To the extent allowed by applicable law, any controversy or claim arising out of or relating to this Agreement or any breach thereof, may be settled by informal mediation with the parties subject to this Agreement.
16. **Compliance with Laws and LEA Board Policy.** Provider, at Provider's sole cost, shall comply with applicable LEA Board Policy as well as all present and future laws, ordinances, rules, regulations, including but not limited to: the Family Educational Rights and Privacy Act ("FERPA") (20 U.S.C. § 1232g; 34 CFR Part 99); Protection of Pupil Rights Amendment ("PPRA") (20 U.S.C. § 1232h; 34 CFR Part 98), all of them which may be in effect or amended from time to time, including any successor statute and its implementing regulations and rules. In the event of a conflict between this Agreement and federal and state confidentiality and privacy laws ("Confidentiality Laws"), the Confidentiality Laws shall control. In the event of a conflict between FERPA and any other Confidentiality Laws, FERPA will control absent clear statutory authority on controlling law.
17. **Children's Online Privacy Protection Act.** The parties recognize and agree that with respect to the Children's Online Privacy Protection Act ("COPPA"), the LEA gives its consent to Provider on behalf of parents of children from whom any personal information shall be gathered, as contemplated under the Agreement. As the agreement only contemplates the potential collection of personal information from children under the age of thirteen (13) for educational purposes, for the use and benefit of the school, and for no other commercial purpose, the parties recognize that COPPA does not require that the Provider obtain consent from parents directly. As such, notwithstanding any other provision in the Agreement to