TPT Student Data Processing Agreement

This Student Data Processing Agreement ("DPA") is entered into between Teacher Synergy LLC (referred to herein as "Provider") and the educational institution or local education agency (referred to herein as the "LEA") identified on the signatory page below, each a "Party" and together the "Parties". This DPA is incorporated into and made part of the applicable Service Agreement (as defined in Exhibit A).

RECITALS

WHEREAS the Provider and the LEA, through their respective employees or agents, have entered into a Service Agreement for the provision of certain digital educational services, as further described herein and in the Service Agreement ("Services"); and

WHEREAS the LEA's use of the Services may result in the Provider receiving and processing Student Data that may be covered by certain federal laws and/or state laws governing the privacy and security of student information, to the extent they apply to LEA or Vendor with respect to the Student Data shared including the Federal Educational Rights and Privacy Act ("FERPA") and the Children's Online Privacy Protection Act ("COPPA").

WHEREAS the Parties recognize the importance of the protection of Student Data and wish to enter into this DPA for the purposes of establishing respective responsibilities regarding the treatment of Student Data.

NOW THEREFORE, for good and valuable consideration, the Parties agree as follows:

I. PURPOSE AND SCOPE

1. **Services.** The Services, as updated from time to time, generally include access to instructional content as well as tools for digital creation, preparation and assignment of materials to students and student access and completion.
2. **Purpose.** The purpose of this DPA is to describe the duties and responsibilities of each Party to protect Student Data transmitted to Provider from the LEA and its users pursuant to the Service Agreement.
3. **Student Data.** In order to provide the Services, Provider may receive Student Data as identified in further detail in the Student Privacy Policy (https://www.teacherspayteachers.com/Student-Privacy-Policy), as amended from time to time.
3. **Definitions.** Capitalized terms used herein shall have the meanings set forth herein or in Exhibit A.
4. **Order of precedence.** As to the subject matter of the protection of Student Data this DPA governs in the event of, and only to the extent of, a direct conflict between this DPA and the Service Agreement. In all other respects the Service Agreement controls and remains in full force and effect.

II. OWNERSHIP AND 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 Parties agree that as between them, all intellectual property rights in and to Student Data, 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.
2. **Parent Access.** LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Student Data and/or correct erroneous information. 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. Provider shall respond in a reasonably timely manner to a request from the LEA's for Student Data in a student's records held by the Provider to view or correct as necessary.
3. **Separate Student Account.** To the extent supported by Provider's Services, at LEA's written request, Provider will assist as necessary in the transfer of Student-Generated Content to separate student created account with Provider.
4. **Third Party Requests.** Should a third party including, but not limited to law enforcement and government entities, contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall redirect the third party to request the data directly from the LEA, unless and to the extent that Provider reasonably believes it must grant such access to the third party because the data disclosure is necessary: (i) pursuant to a court order or legal process, (ii) to comply with statutes or regulations, (iii) to enforce the Agreement, or (iv) if Provider believes in good faith that such disclosure is necessary to protect the rights, property or personal safety of Provider's users, employees or others. Provider shall notify the LEA in advance of a compelled disclosure to a third party, unless legally prohibited.
5. **Subprocessors.** Provider may engage the services of Subprocessors in order to provide the Services. Provider agrees that any Subprocessors it uses to process Student Data employs security protections as stringent as those described in Section IV.1, are bound by confidentiality provisions consistent with this DPA, and will only process Student Data for purposes of providing its services to Provider.

III. DUTIES OF THE LEA

1. **Compliance with Applicable Laws.** LEA shall provide Student Data in compliance with any applicable state or federal laws and regulations pertaining to data privacy and security. LEA represents and warrants, as applicable, that LEA has:
   a. complied with the school official exemption under FERPA, including, without limitation, informing parents in their annual notification of FERPA rights that the Institution defines "school official" to include service providers and defines "legitimate educational interest" to include services such as the type provided by Provider; and

b. obtained all necessary parental or eligible student written consent to share the Student Data with Provider.

2. **Reasonable Security.** LEA will maintain administrative, physical, and technical safeguards consistent with industry standards designed to protect usernames, passwords, and any other means of gaining access to the Services ("User Credentials") from unauthorized access, disclosure or acquisition by an unauthorized person.
3. **Notice of Unauthorized Access.** LEA agrees to notify Provider immediately in the event that (i) LEA believes that any unauthorized access to the Services has occurred; (ii) LEA believes that the confidentiality of any User Credentials used with the Services have been compromised; and/or (iii) any User Credentials no longer in use need to be disabled. LEA will assist Provider in any efforts by Provider to investigate and respond to potential unauthorized access.

IV. DUTIES OF THE PROVIDER

1. Compliance with Applicable Laws. The Provider shall comply in all material respects with state and federal laws and regulations pertaining to Student Data privacy and security, applicable to the Provider in providing the Service to LEA.

2. **Responsibility of Employees.** Provider is responsible for ensuring that its employees and contractors who may access Student Data as part of their job duties for Provider abide by the terms of this DPA.

3. **No Disclosure**. Provider will not sell Student Data to any third party and Provider will not disclose, transfer, share or rent any Student Data obtained under hereunder in a manner that directly identifies an individual student to any other entity other than LEA, except: (i) as authorized under this DPA; (ii) as directed by LEA; (iii) to authorized users of the Services (including as applicable, LEA's account holders, and/or students' parents or legal guardians); (iv) as permitted by law; (v) in response to a legal order; (vi) to protect the safety or integrity of users or others, or the security of the Services; or (vii) to Subprocessors, in connection with operating the Services.

4. Limited Use. Student Data shared pursuant to this Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services and for the uses set forth in the Service Agreement and this DPA and/or as otherwise legally permissible, including, without limitation, for adaptive learning or customized student learning. The foregoing limitation does not apply to any De-Identified Information.

5. Advertising Limitations. Provider is prohibited from using Personally Identifiable Information contained in Student Data to (a) serve Targeted Advertising to students or families/guardians; (b) develop a profile of a student for any commercial purpose other than providing the Service or as authorized by the parent/guardian or LEA; or (c) develop commercial products or services, other than as necessary to provide the Service to LEA, as authorized by the parent or legal guardian, or as permitted by applicable law. This section shall not be construed to (i) limit the ability of Provider to use Student Data for adaptive learning or customized student learning purposes (including generating personalized learning recommendations for account holders or sending Program Communications to account holders); (ii) prohibit Provider from using aggregate or De-Identified Information to inform, influence or enable marketing, advertising or other commercial efforts by Provider, (iii) prohibit Provider from marketing or advertising directly to parents/guardians or other users so long as the marketing or advertising did not result from the use of Personally Identifiable Information contained in Student Data obtained by Provider from providing the Services; (iv) prohibit Provider from using Student Data to make recommend relevant uses, features, educational resources or other offerings from Provider's Services to parents/guardians or LEA's users.

6. **De-Identified Information.** De-Identified Information may be used by the Provider for any lawful purpose, including, but not limited to, development, research, and improvement of educational sites, services, or applications, and to demonstrate the market effectiveness of the Services. Provider's use of such De-Identified Information shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Provider agrees not to attempt to re-identify De-identified Information and not to transfer De-Identified Information to any party unless that party agrees in writing not to attempt re-identification.
7. **Disposition.** Provider will only retain Student Data as long as reasonably necessary for the purpose for which it was collected. Except for Student Generated Content transferred to a separate student account in accordance with Article II Section 3, upon written request from the LEA, Provider will dispose of all Personally Identifiable Information contained in the Student Data within a reasonable time period following such written request and provide written notification to LEA to confirm completion of the requested disposition. If no written request is received, Provider shall dispose of or delete all Personally Identifiable Information contained in Student Data when it is no longer needed for the purpose for which it was obtained. Disposition shall include (1) the shredding of any hard copies; (2) erasing; or (3) otherwise modifying the Personally Identifiable Information contained in Student Data to make it unreadable or indecipherable. The duty to dispose of Student Data shall not extend to De-Identified Information.

V. DATA PROTECTION

1. **Reasonable Security.** Provider agrees to maintain reasonable administrative, physical, and technical safeguards consistent with industry standards designed to protect against the unauthorized access, disclosure or acquisition of Student Data. The specific security duties of Provider are set forth below.
   a. **Storage in the US.** Provider agrees that Student Data shall be stored on servers located in the United States.
   b. **Password protected access.** Access to the Services and to Student Data by LEA's users and Provider's employees and contractors shall be secured through authentication protocols designed to ensure that Student Data may only be viewed or accessed by parties legally allowed to do so.
   c. **Employee Training.** The Provider shall provide periodic security training to those of its employees who operate or have access to the Services.
   d. **Security Technology.** When the Service is accessed using a supported web browser, Transport Layer Security ("TLS"), or equivalent technology shall be employed to protect Student Data when in transit. Student Data stored within our platform is encrypted at rest. Provider will host Student Data pursuant in an environment protected using firewalls that are maintained according to industry standards.

e. **Access controls.** Provider shall limit internal access to Student Data to employees or contractors requiring access in performance of their job duties and to Subprocessors that are necessary in performance of the Services.

f. **Periodic assessment.** Provider further acknowledges and agrees to conduct periodic assessments of the security of the Services, including security audits, risk assessments, and/or penetration tests and remediate any critical security and privacy vulnerabilities in a timely manner.

g. **Disposal.** Personally Identifiable Information contained in the Student Data shall be securely disposed of in accordance with Article IV Section 5.

2. **Data Breach.** In the event of a breach of Provider's security that results in an unauthorized release, disclosure or acquisition of Personally Identifiable Information contained in the Student Data ("Security Breach"), Provider will notify impacted users without undue delay and in accordance with applicable state law after becoming aware of the Security Breach.

   a. **Notice.** Unless otherwise required by the applicable law, the Security Breach notification will be written in plain language and will present the following details: what happened, what information was involved, what we are doing, what you can do, and how to request more information. The breach notification will include the following information, to the extent available or known:

      i. A name and contact information for the Provider;

      ii. A list of the types of personal identifiable information that were or are reasonably believed to have been the subject of the Security Breach;

      iii. The date, estimated date, or time range within which the Security Breach is believed to have occurred; and

      iv. A general description of the Security Breach, if that information is possible to determine at the time the notice is provided.

   b. **Compliance with laws.** Provider agrees to adhere to all requirements applicable to Provider providing the Service in applicable State and federal law with respect to a Security Breach, including any required responsibilities and procedures for notification and mitigation of any such Security Breach.

   c. **Incident Response Plan.** Provider further acknowledges and agrees to have a written incident response plan consistent with industry standards and federal and state law for responding to a Security Breach and agrees to provide LEA, upon request, with a copy of the Incident Response Plan or a summary of such Incident Response Plan to the extent such plan includes sensitive or confidential information of Provider.

VI. MISCELLANEOUS

1. **Term.** This DPA shall remain in effect for the duration of the Service Agreement.
2. **Termination**. The LEA or Provider may terminate this DPA and the Service Agreement in the event of a material breach of the terms of this DPA.
3. **Effect of Termination.** If this DPA and the Service Agreement are terminated, the Provider shall dispose of all of Personally Identifiable Information contained in Student Data in accordance with the procedures set forth in Article IV Section 5.

4. **Amendment.** This DPA may be amended 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. For clarity, nothing in this Section prohibits Provider from amending the Service Agreement pursuant to the amendment provisions set forth therein.
5. **Severability.** Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective only 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. **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 prior to the transfer of any Student Data to such successor.

Signatures next page

Signatory Information

By signing below, I accept this DPA on behalf of the LEA. I represent and warrant that (a) I have full legal authority to bind the LEA to this DPA, (b) I have read and understand this DPA, and (c) I agre to all terms and conditions of this DPA on behalf of the LEA that I represent.

LEA Information:

Name of LEA: Rose Bud School District

LEA Address: 124 School Rd. Rose Bud, AR 72137

LEA Authorized Representative:

Signature: A. Turley

Name: Alicia Turley

Title: Director of Technology

Email: aturley@rbsd.k12.ar.us

Date: 8 Feb 2024

Teacher Synergy LLC Authorized Representative:

Signature: Paul Mishkin

Name: Paul Mishkin

Title: Chief Executive Officer

Email: privacy@teacherspayteachers.com

Date: 12/21/2023

EXHIBIT A: DEFINITIONS

1. **"De-Identified Information"** means records and information when all Personally Identifiable Information has been removed or obscured, such that the remaining information does not reasonably identify a specific individual.
2. **"Personally Identifiable Information"** means information that can be used alone or in combination with other information to identify a particular individual including persistent identifiers. Information that has been De-identified or aggregated and anonymous usage data are not considered Personally Identifiable Information.
3. **"Program Communications"** means in-app or emailed communications relating to Provider's educational services, including prompts, messages and content relating to the use of the Service, for example; onboarding and orientation communications, prompts for students to complete, or teachers to assign exercises or provide feedback as part of the learning exercise, periodic activity reports, suggestions for additional learning activities in the Service, service updates.
4. **"Service Agreement"** means Provider's Terms of Service, Subscription Agreement and any incorporated agreements or policies. Service Agreement also includes any Provider issued ordering document or invoice.
5. **"Student Data"** means any Personally Identifiable Information that is descriptive of the student, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians for a school purpose, pursuant to LEAs use of the Services, including as applicable first and last name, home address, telephone number, email address, or other information allowing online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information, text messages, school ID, photos, voice recordings or geolocation information. Student Data may include "education records" as defined under FERPA. Student Data shall not include De-Identified Information or information that has been anonymized or aggregated or anonymous usage data regarding a student's use of Provider's Service.
6. **"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.
7. **"Subprocessors"** 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 Services.
8. **"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 Provider's 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 based on the content of the web page, search query, or in response to a student's response or request for information or feedback.

EXHIBIT B: STATE SPECIFIC TERMS

To the extent not already covered by this DPA, TpT will comply with the applicable requirements of the following state laws governing the collection and use of Student Data:

New York — New York Education Law § 2-d (NY-2d). TpT does not collect “teacher and principal data” as that term is defined under NY-2d, but to the extent TpT receives or processes such information at any future time, TpT will protect the confidentiality of such data in accordance with the requirements of NY-2d. TpT agrees to attach and incorporate your Parents’ Bill of Rights as part of this DPA.

California – SB-1177 SOPIPA.

Connecticut – Public Act No. 16-189 and Conn. Gen. Stat. 10-234aa-dd.

I**llinois** — 105 ILCS 85 SOPPA.

Maine - SP0183, Maine's Student Information Privacy Act.