KIDREWARDS STUDENT DATA PRIVACY ADDENDUM[1]

This Student Data Privacy Addendum ("DPA") is incorporated by reference into the Service Agreement (as defined below) entered into by and between the educational agency set forth below (hereinafter referred to as "LEA") and KidRewards (hereinafter referred to as "Provider") effective as of the date the DPA is accepted by LEA ("Effective Date") (each of Provider and LEA, a "Party" and together "Parties"). The Parties agree to the terms as stated herein.

This Student Data Privacy Addendum ("DPA") is incorporated by reference into the Service Agreement (as defined below) entered into by and between the educational agency set forth below (hereinafter referred to as "LEA") and KidRewards (hereinafter referred to as "Provider") effective as of the date the DPA is accepted by LEA ("Effective Date") (each of Provider and LEA, a "Party" and together "Parties"). The Parties agree to the terms as stated herein.

RECITALS

WHEREAS, the Provider has agreed or will agree to provide the LEA with certain digital educational services as described in Section 1 pursuant to the KidRewards Terms of Service located at https://www.kidrewards.org/terms.html (the "Service Agreement"); and

WHEREAS, in order to provide the Services described in Section 1, the Provider may receive or create and the LEA may provide documents or data that are covered by several federal statutes, among them, the Family Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. 1232g and 34 CFR Part 99, Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. 6501-6502; Protection of Pupil Rights Amendment ("PPRA") 20 U.S.C. 1232h; the Individuals with Disabilities Education Act ("IDEA"), 20 U.S.C. §§ 1400 et. seq.; and

WHEREAS, the documents and data transferred from LEAs and created or accessed by the Provider's Services are also subject to various state student privacy laws; and

WHEREAS, the Parties wish to enter into this DPA to ensure that the Services and Service Agreement provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties.

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

1. PURPOSE AND SCOPE

1.1. **Purpose of DPA**. The purpose of this DPA is to describe the duties and responsibilities to protect Student Data (as defined in Exhibit "C") transmitted to Provider from the LEA and it's users pursuant to the Service Agreement including compliance with all applicable federal and state privacy statutes, including the FERPA, PPRA, COPPA, and IDEA. This DPA supplements the Service Agreement and together with the Service Agreement, is collectively referred to as the "Agreement".

1.2. **Nature of Services Provided.** Pursuant to and as fully described in the Service Agreement, Provider has agreed to provide the digital educational services as set forth in Exhibit "A" hereto and any other products and services that Provider may provide now or in the future (the "Services").

1.3. **Student Data to Be Provided.** In order to perform the Services, the Parties shall indicate the categories of Student Data to be provided or collected by the Provider in the Schedule of Data, attached hereto as Exhibit "B".

1.4. **DPA Definitions.** The definition of terms used in this DPA is found in Exhibit "C". In the event of a conflict, definitions used in this DPA shall prevail over terms used in all other writings, including, but not limited to, the Service Agreement, privacy policies or any terms of service with respect to the treatment of Student Data.

2. DATA OWNERSHIP AND AUTHORIZED ACCESS

2.1. **Student Data Property of LEA**. All Student Data or any other Education Records (as defined on Exhibit "C") transmitted to the Provider pursuant to this Agreement is and will continue to be the

[1] Modeled After The Student Data Privacy Consortium's Set Of Baseline Model Clauses

property of and under the control of the LEA, or to the party who provided such data (such as the student or parent.). The Provider further acknowledges and agrees that all copies of such Student Data or Education Records transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are also subject to the provisions of this Agreement in the same manner as the original Student Data or Education Records. The Parties agree that as between them, all rights, including all intellectual property rights, in and to Student Data or Education Records covered per this Agreement shall remain the exclusive property of the LEA or the party who provided such data (such as the student or parent).

2.2. **Exemptions under FERPA**. LEA may not generally disclose Personally Identifiable Information from an eligible student's Education Record to a third-party without written consent of the parent and/or eligible student or without meeting one of the exemptions set forth in FERPA ("FERPA Exemption(s)"), including the exemption for Directory Information ("Directory Information Exemption") or School Official exemption ("School Official Exemption"). For the purposes of FERPA, to the extent Personally Identifiable Information from Education Records are transmitted to Provider from LEA or from students using accounts at the direction of the LEA, the Provider shall be considered a School Official (as defined on Exhibit "C"), under the control and direction of the LEAs as it pertains to the use of Education Records. Additionally, certain information, provided to Provider by LEA about a student, such as student name and grade level, may be considered Directory Information (as defined on Exhibit "C") under FERPA and thus not an Education Record.

2.3. **Parent Access**. LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Personally Identifiable Information contained in the related student's Education Records and correct erroneous information, consistent with the functionality of Services. Provider shall cooperate and respond within thirty (30) days to the LEA's request for Personally Identifiable Information contained in the related student's Education Records held by the Provider to view or correct as necessary. In the event that a parent/legal guardian of a student or other individual contacts the Provider to review any of the Education Records or 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, provided however, that Provider may also allow for direct access requests (but not correction or deletion rights) of Student Data and/or Education Records from a verified parent.

2.4. **Separate Account**. Students and parent users may have personal or non-school accounts (i.e. for use of KidRewards at home not related to school) in addition to school accounts ("Outside School Account(s)"). An Outside School Account of a student may also be linked to their student account. Student Data shall not include information a student or parent provides to Provider through such Outside School Accounts independent of the student's or parent's engagement with the Services at the direction of the LEA. Additionally, If Student Generated Content is stored or maintained by the Provider as part of the Services, Provider may, at the request or with the consent of the parent or legal guardian, transfer said Student Generated Content to a separate student account or the Outside School Account upon termination of the Service Agreement; provided, however, such transfer shall only apply to Student Generated Content that is severable from the Service.

2.5. **Third Party Request**. Should a third party, excluding a Service Provider, including, but not limited to law enforcement, former employees of the LEA, current employees of the LEA, 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.

2.6. **Service Providers**. Provider shall enter into written agreements with all Service Providers performing functions pursuant to this Agreement, whereby the Service Providers agree to protect Student Data in manner no less stringent than the terms of this DPA. The list of Provider's current Service Providers can be accessed through the Provider's Privacy Policy (which may be updated from time to time).

3. DUTIES OF LEA

3.1. **Provide Data In Compliance With Laws**. LEA shall provide Student Data for the purposes of the Agreement in compliance with any applicable state or federal laws and regulations pertaining to data privacy and security, including, without limitation, the FERPA, PPRA, and IDEA. If LEA is providing Directory Information or any Education Record to Provider, LEA represents, warrants and covenants to Provider, as applicable, that LEA has:

a. complied with the Directory Information Exemption, including, without limitation, informing parents and eligible students what information the LEA deems to be Directory Information and may be disclosed and allowing parents and eligible students a reasonable amount of time to request that schools not disclose Directory Information about them; and/or

b. complied with the School Official Exemption, 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; or

c. obtained all necessary parental or eligible student written consent to share the Student Data with Provider, in each case, solely to enable Provider's operation of the Service.

If LEA is relying on the Directory Information exemption, LEA represents, warrants, and covenants to Provider that it shall not provide information to Provider from any student or parent/legal guardian that has opted out of the disclosure of Directory Information. Provider depends on LEA to ensure that LEA is complying with the FERPA provisions regarding the disclosure of any Student Data that will be shared with Provider.

3.2. **Reasonable Security**. LEA shall employ administrative, physical, and technical safeguards consistent with industry standards designed to protect usernames, passwords, and any other means of gaining access to the Services and/or hosted data from unauthorized access, disclosure or acquisition by an unauthorized person.

3.3. **Unauthorized Access Notification**. LEA shall notify Provider immediately, but in no less than 72 hours, of any known or suspected unauthorized use or access of the Services, LEA's account, or Student Data. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized use or access.

4. DUTIES OF PROVIDER

4.1. **Privacy Compliance**. The Provider shall comply in all material respects with all applicable state and federal laws and regulations pertaining to data privacy and security, applicable to the Provider in providing the Service to LEA. With respect to Student Data that the LEA permits Provider to collect or access pursuant to the Agreement, Provider agrees to support LEA in upholding LEA's responsibilities with FERPA and PPRA.

4.2. **AuthorizedUse**. Student Data shared pursuant to this Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services and for the uses set forth in the Agreement 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 Data (as defined in Exhibit "C").

4.3. **Employee Obligation**. Provider shall require all 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 this DPA. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the DPA.

4.4. **No Disclosure**. Provider shall not disclose, transfer, share or rent any Student Data obtained under the Agreement in a manner that directly identifies an individual student to any other entity other than LEA, except: (i) as authorized by the Agreement; (ii) as directed by LEA; (iii) to authorized users of the Services, including parents or legal guardians; (iv) as permitted by law; (v) in response to a judicial order as set forth in Section 2.5; (vi) to protect the safety or integrity of users or others, or the security of the Services; or (vii) to Service Providers, in connection with operating or improving the Service. Provider will not Sell (as defined in Exhibit "C") Student Data to any third party.

4.5. **De-Identified Data**. De-Identified Data 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 Data 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 Data and not to transfer De-identified Data to any party unless that party agrees in writing not to attempt re-identification.

4.6. **Disposition of Data**. Provider shall, at LEA's request, dispose of or delete all Personally Identifiable Information contained in Student Data within a reasonable time period following a written request. If no written request is received, Provider shall dispose of or delete all Personally Identifiable Information contained in Student Data at the earliest of (a) when it is no longer needed for the purpose for which it was obtained or (b) as required by applicable law. Nothing in the DPA authorizes Provider to maintain Personally Identifiable Information contained in Student Data obtained under the Agreement beyond the time period reasonably needed to complete the disposition, unless a student, parent or legal guardian of a student chooses to establish and maintain a separate account with Provider to retain Student Generated Content. Disposition shall include (1) the shredding of any hard copies of any Personally Identifiable Information contained in Student Data; (2) erasing any Personally Identifiable Information contained in Student Data; or (3) otherwise modifying the Personally Identifiable Information contained in Student Data to make it unreadable or indecipherable or De-Identified or placed in a separate student account, pursuant to the other terms of the DPA. Provider shall provide written notification to LEA when the Personally Identifiable Information contained in Student Data has been disposed pursuant to the LEA's request for deletion. The duty to dispose of Student Data shall not extend to data that has been De-Identified. The LEA may employ a "Request for Return or Deletion of Student Data" substantially in the form attached hereto as Exhibit "D".

4.7. **Transfer of Student Data to LEA**. If a written request is received from LEA to transfer Personally Identifiable Information contained in Student Data to LEA, Provider shall transfer said Personally Identifiable Information contained in Student Data to LEA or LEA's designee within sixty (60) days of the date of such written request by LEA, or as required by law, and according to a schedule and procedure as the Parties may reasonably agree.

4.8. **Advertising Prohibition**. Provider is prohibited from using Personally Identifiable Information contained in Student Data to (a) serve Targeted Advertising to students or families/guardians unless with the consent of parent/guardian or LEA; (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 Data to inform, influence or enable marketing, advertising or other commercial efforts by Provider, (iii) prohibit Provider from marketing or advertising directly to

parents 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 recommend educational products or services to parents/guardians, students or LEA's so long as the recommendations are not based in whole or part by payment or other consideration from a third party; (v) apply to the marketing of school memorabilia such as photographs, yearbooks, or class rings or (vi) prohibit Provider from using Student Data with parent/guardian consent to direct advertising to students to identify higher education or scholarship providers that are seeking students who meet specific criteria.

5. DATA SECURITY AND DATA BREACH

5.1. **Data Security**. The Provider agrees to employ administrative, physical, and technical safeguards consistent with industry standards designed to protect Student Data from unauthorized access, disclosure, use or acquisition by an unauthorized person, including when transmitting and storing such information. The general security duties of Provider are set forth below. Provider may further detail its security programs and measures in Exhibit "E" hereto. These measures shall include, but are not limited to:

a. **Passwords and Employee Access**. Provider shall secure usernames, passwords, and any other means of gaining access to the Services or to Student Data, at a level consistent with Article 4.3 of NIST 800-63-3. Provider shall only provide access to Student Data to employees, contractors or Service Providers that are performing the Services.

b. **Security Protocols**. Both parties agree to maintain security protocols that meet industry best practices in the transfer or transmission of any Student Data, including ensuring that Student Data may only be viewed or accessed by parties legally allowed to do so. Provider shall maintain all Student Data obtained or generated pursuant to the Agreement in a secure computer environment and not copy, reproduce, or transmit Student Data obtained pursuant to the Agreement except as necessary to provide the Service, to fulfill data requests by LEA or as otherwise set forth in the Agreement. The foregoing does not limit the ability of the Provider to disclose information as permitted under Section 2.5 or to allow any necessary Service Providers to view or access data as set forth in Section 4.4.

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, Secure Socket Layer ("SSL"), or equivalent technology shall be employed to protect Student Data from unauthorized access. The security measures employed shall include server authentication and data encryption at rest and in transit. Provider shall host Student Data pursuant to the Agreement in an environment using a firewall that is maintained according to industry standards.

e. **Security Coordinator**. The name and contact information of each Party's designated representative for the purposes of matters relating to security of Student Data received pursuant to the Agreement is set forth below:

i. Provider's security coordinator ("Security Coordinator") is: Naveed Ahmed, contact@kidrewards.org.

ii. LEA's designated representative of matters relating to security of Student Data is set forth on the signature page of this DPA.

f. **Service Provider Bound**. Provider shall enter into written agreements whereby Service Providers agree to secure and protect Student Data in a manner no less stringent than the terms of this Section 5. Provider shall periodically conduct or review compliance monitoring and assessments of Service Providers to determine their compliance with this Section 5.

g. **Periodic Risk Assessment**. Provider further acknowledges and agrees to conduct periodic risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner.

5.2. **Data Breach**. In the event that Provider becomes aware of any actual or reasonably suspected unauthorized disclosure of or access to Student Data (a "Security Incident"), Provider shall provide notification to LEA as required by the applicable state law, but in no event later than thirty (30) days of the incident (each a "Security Incident Notification") Provider shall follow the following process:

a. Unless otherwise required by the applicable law, the Security Incident Notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described herein under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.

b. The Security Incident Notification described above in section 5.2(a) shall include such information required by the applicable state law, and at a minimum, the following information, to the extent available:

i. The name and contact information of the reporting Provider subject to this section.

ii. A list of the types of Personal Identifiable Information that were or are reasonably believed to have been the subject of the Security Incident.

iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the Security Incident, (2) the estimated date of the Security Incident, or (3) the date range within which the Security Incident occurred. The Security Incident Notification shall also include the date of the notice.

iv. Whether, to the knowledge of Provider at the time the Security Incident Notice was provided the notification was delayed as a result of a law enforcement investigation

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

c. At Provider's discretion, the Security Incident Notification may also include any of the following:

i. Information about what the Provider has done to protect individuals whose Personally Identifiable Information has been breached by the Security Incident.

ii. Advice on steps that the person whose Personally Identifiable Information has been breached may take to protect himself or herself.

d. Provider agrees to adhere to all requirements applicable to Provider providing the Service in applicable State and federal law with respect to a Security Incident related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such Security Incident.

e. 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 Security Incident involving Student Data or any portion thereof, including Personally Identifiable Information ("Incident Response Plan") 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.

f. To the extent LEA determines that the Security Incident triggers third party notice requirements under applicable laws, Provider will cooperate with LEA as to the timing and

content of the notices to be sent. Except as otherwise required by law, Provider will not provide notice of the Security Incident directly to individuals whose Personally Identifiable Information was affected, to regulatory agencies, or to other entities, without first providing written notice to LEA. This provision shall not restrict Provider's ability to provide separate security breach notification to customers, including parents and other individuals with Outside School Accounts.

6. MISCELLANEOUS

6.1. **Term**. The Provider shall be bound by this DPA for the duration of the Service Agreement or as required by law.

6.2. **Termination**. In the event that either party seeks to terminate this DPA, they may do so by terminating the Service Agreement as set forth therein. 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.

6.3. **Effect of Termination Survival**. If the Service Agreement is terminated (thereby terminating this DPA), the Provider shall dispose of all of LEA's Personally Identifiable Information contained in Student Data following the procedures set forth in Section 4.6, which includes De-Identification.

6.4. **Priority of Agreements**. This DPA shall govern the treatment of Student Data. With respect to the treatment of Student Data, in the event there is conflict between the terms of the DPA, the Service Agreement, or any other agreement between Provider and LEA, the terms of this DPA shall apply and take precedence. Except as described in this paragraph herein, all other provisions of the Service Agreement, or any other agreement shall remain in effect, including, without limitation, any license rights, limitation of liability or indemnification provisions.

6.5. **Notice**. All notices or other communication required or permitted to be given hereunder must be in writing and given by personal delivery, facsimile or e-mail transmission (if contact information is provided for the specific mode of delivery), or first class mail, postage prepaid, sent to the designated representatives before:

- **a.** The designated representative for the Provider for this DPA is: Naveed Ahmed, contact@kidrewards.org.
- **b.** The designated representative for the LEA for this DPA is the individual who enters into the DPA and provides his or her relevant email address (online) during the acceptance process.

6.6. **Entire Agreement**. This DPA constitutes the entire agreement of the parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both parties. Neither failure nor delay on the part of any party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege. For clarity, nothing in this Section prohibits Provider from amending the Service Agreement pursuant to the amendment provisions set forth therein.

6.7. **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.

6.8. **Governing Law; Venue and Jurisdiction**. THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE LEA SIGNING THE DPA, 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 THE LEA RESIDES IN, OF THE STATE OF THE LEA SIGNING THE DPA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.

6.9. **Waiver**. No delay or omission of the LEA or Provider to exercise any right hereunder shall be construed as a waiver of any such right and the LEA or Provider (as applicable) reserves the right to exercise any such right from time to time, as often as may be deemed expedient.

6.10. **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.

6.11. **Electronic Signature**: The Parties understand and agree that they have the right to execute this Agreement through paper or through electronic signature technology, which is in compliance with applicable state and Federal law governing electronic signatures. The parties agree that to the extent they sign electronically, their electronic signature is the legally binding equivalent to their handwritten signature. Whenever they execute an electronic signature, it has the same validity and meaning as their handwritten signature. They will not, at any time in the future, repudiate the meaning of their electronic signature or claim that their electronic signature is not legally binding. They agree not to object to the admissibility of this Agreement as an electronic record, or a paper copy of an electronic document, or a paper copy of a document bearing an electronic signature, on the grounds that it is an electronic record or electronic signature or that it is not in its original form or is not an original.

7. EU GENERAL DATA PROTECTION REGULATION (GDPR). To the extent that LEA is an entity located in the EEA, the following additional provisions shall apply.

7.1. **Roles.** LEA is a Controller and appoints Provider as a Processor of Student Data on behalf of LEA.

7.2. **Scope.** This DPA applies to Processing of Student Data by Provider on behalf of LEA and in accordance with LEA's instructions as part of the Services described in the Agreement. The subject matter, nature and purpose of the Processing, the types of Student Data and categories of Data Subjects are set out in Exhibit "B".

7.3. **Instructions.** Provider must only Process Student Data on documented instructions of LEA, and is prohibited from Processing Student Data for any other purpose. LEA's instructions are set forth in the Agreement. LEA may issue additional instructions to Provider as it deems necessary to comply with Data Protection Law. The authorized use is as set forth in Section 4.2 ("Authorized Use") above. Instructions may only be issued by the LEA's management board, data protection officers or the manager of the LEA's legal department, if applicable.

7.4. **Subprocessing.** LEA hereby authorizes Provider to engage the Subprocessors listed in Provider's Privacy Policy (which may be updated from time to time). Provider must enter into a written agreement with all Subprocessors as set forth in Section 2.6 ("Service Providers") above. Provider must obtain sufficient guarantees from all Subprocessors that they will implement appropriate technical and organizational measures in such a manner that the Processing will meet the requirements of Data Protection Law and this DPA.

7.5. **International Data Transfers.**

a. LEA hereby authorizes Provider to perform International Data Transfers to countries subject to a current adequacy decision of the EU Commission, and to perform the specific

International Data Transfer(s) listed in Exhibit "B". Notwithstanding anything to the contrary in this DPA or the Agreement, LEA acknowledges and agrees that Provider may store Student Data in various data centers around the world, and that Student Data might not be hosted within the country in which LEA is located.

b. All authorizations of International Data Transfers pursuant to Section 7.5 are expressly conditioned upon Provider's ongoing compliance with the requirements of Data Protection Law applicable to International Data Transfers, and any applicable legal instrument for International Data Transfers. If such compliance is affected by circumstances outside of Provider's control, including the amendment, replacement or annulment of applicable legal instruments, LEA and Provider will work together in good faith to reasonably resolve such non-compliance.

c. To the extent Provider Processes Personal Data that is covered by LEA's certification to the EU-U.S. or Swiss-U.S. Privacy Shield framework:

i Provider must maintain a certification to the same Privacy Shield framework or provide at least the same level of privacy protection as is required by the Privacy Shield principles;

ii Provider must notify LEA if it determines that it can no longer meet its obligation to provide at least the same level of protection as is required by the Privacy Shield principles, in which case LEA may take all appropriate steps to stop and remediate unauthorized Processing.

7.6. Personnel. Provider must implement appropriate technical and organizational measures to ensure that Personnel do not Process Personal Data except on the instructions of the Controller and will follow additional obligations at set forth in Section 4.3 ("Employee Obligations") and Section 5.1(a) ("Passwords and Employee Access") and Section 5.1 (c) ("Employee Training").

7.7. Confidentiality. Provider must keep all Student Data and any information relating to the Processing thereof, in strict confidence as set forth in Section 4.4 ("No Disclosure").

7.8. Security and Personal Data Breaches.

a. Provider must implement technical and organizational measures to ensure a level of security appropriate to the risks presented by the Processing, including encryption and pseudonymization of Student Data as set forth in Section 5.1 ("Data Security") and, as appropriate and without limiting the foregoing, the measures listed in Exhibit "E".

b. Provider must inform LEA without undue delay after becoming aware of a Personal Data Breach of Student Data of LEA and will follow the procedures set forth in Section 5.2 ("Data Breach").

7.9. Assistance.

a. Provider must provide reasonable assistance to LEA with the fulfilment of LEA's own obligations under Data Protection Law with respect to: 1) complying with Data Subjects' requests to exercise Data Subject Rights, 2) replying to inquiries or complaints from Data Subjects, 3) replying to investigations and inquiries from Supervisory Authorities, 4) notifying Personal Data Breaches of LEA's Student Data, and 5) prior consultations with Supervisory Authorities. Provider will follow the procedures set forth in Section 2.3 ("Parent Access").

b. Upon reasonable request, Provider must provide LEA with all information necessary to enable LEA to satisfy notification obligations, maintaining records of Processing activities, or performing a data protection impact assessment.

c. Provider must promptly inform LEA if Provider believes that an instruction of LEA violates

Data Protection Law.

d. Unless prohibited by EU or EU member state law and subject to the procedures set forth in Section 2.5 above, ("Third-Party Request"). Provider must promptly inform LEA if Provider: receives a request to disclose Personal Data from law enforcement, courts or any government entity; is subject to a legal obligation that requires Provider to Process Personal Data in contravention of LEA's instructions; or is otherwise unable to comply with Data Protection Law or this DPA.

e. If Provider is prevented from notifying LEA as required under or this DPA, Provider must consult and comply with the instructions of the competent Supervisory Authority.

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 agree to all terms and conditions of this DPA on behalf of the LEA that I represent.

Name of LEA: _____

Address: _____

Country: _____

LEA Authorized Representative full name: _____

Title: _____

Email: _____

LEA Authorized Representative signature: _____

Date: _____

Per section 2.3, LEA's contact for parent inquiries:

Name & Email: _____

Title: _____

Per section 5.1(e) LEA's designated representative of matters relating to security of Student Data:

Name & Email: _____

Title: _____

- - - - - -

KidRewards Representative signature: _____

Authorized Representative full name: _____

Title: _____

Email: contact@kidrewards.org

Address: 12830 Hillcrest Rd. #111 Dallas, TX - 75230, U.S.A

Date: _____

EXHIBIT "A"

DESCRIPTION OF SERVICES

KidRewards is an online platform that helps bring teachers, school leaders, families, and students together.

KidRewards provides the following through its platform:

- An online rewards chart to monitor children's progress on various goals
- Feedback and messaging on progress of these goals
- Link to prize on amazon on completion of goals

More information on how the Service operates is located at www.kidrewards.org.

EXHIBIT "B"

SCHEDULE OF DATA**

Category of Data	Elements	Check if used by your system
Application Technology Metadata	IP Addresses of users, Use of cookies etc.	✓
	Other metadata: cookies, local storage, web-beacons, pixel tags	✓
Application Use Statistics	Metadata on user interaction with application	✓
Assessment	Standardized test scores	N/A
	Observation data	✓
	Other assessment data-Please specify:	N/A
Attendance	Student school (daily) attendance data	N/A
	Student class attendance data	✓ if teachers elect to record
Communications	Online communications that are captured (emails, blog entries)	✓ Not from students, unless they message directly with their teacher
Biometric Data	Physical or behavioral human characteristics to can be used to identity a person (e.g. fingerprint scan, facial recognition)	N/A
Conduct	Conduct or behavioral data *For KidRewards: "points/stars" are added by the student's teacher, parent or student*	√
Demographics	Date of Birth *For KidRewards: This is collected as age, not DOB*	√
	Place of Birth	N/A
	Gender	NA/
	Ethnicity or race	N/A
	Language information (native, preferred or primary language spoken by student) *For KidRewards: This is obtained via browser/device preferences*	√
	Other demographic information	N/A
Enrollment	Student school enrollment	√
	Student grade level	√
	Homeroom	N/A
	Guidance counselor	N/A
	Specific curriculum programs	N/A
	Year of graduation	N/A
	Other enrollment information-Please specify:	N/A
Parent/Guardian Contact Information	Address	N/A
	Email	√
	Phone	N/A
Parent/Guardian ID	Parent ID number (created to link parents to students)	√
Parent/Guardian Name	First and/or Last	√
Transcript	Student course grades	N/A
	Student course data	N/A
	Student course grades/performance scores	N/A
	Other transcript data -Please specify:	N/A

Category of Data	Elements	Check if used by your system
Schedule	Student scheduled courses	N/A
	Teacher names	✓
Special Indicator	English language learner information	N/A
	Low income status	N/A
	Medical alerts	N/A
	Student disability information	N/A
	Specialized education services (IEP or 504)	N/A
	Living situations (homeless/foster care)	N/A
	Other indicator information-Please specify:	N/A
Student Contact Information	Address	N/A
	Email	✓ only for students whose teachers elect to enter student emails
	Phone	N/A
Student Identifiers	Local (School district) ID number	N/A
	State ID number	N/A
	Vendor/App assigned student ID number	✓
	Student app username	✓
	Student app passwords	✓
Student Name	First and/or Last *For KidRewards: option to only share last initial*	✓
Student In App Performance	Program/application performance (e.g., typing/reading program performance)	✓ We track points assigned to students
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	N/A
Student Survey Responses	Student responses to surveys or questionnaires	N/A
Student work	Student generated content; writing, pictures etc.	✓
Transportation	Student bus assignment	N/A
	Student pick up and/or drop off location	N/A
	Student bus card ID number	N/A
	Other transportation data - Please specify:	N/A
Other	Please list each additional data element used, stored or collected by your application	

EXHIBIT "C"

DEFINITIONS

"De-Identified Data" means information that has all Personally Identifiable Information, including direct and indirect identifiers removed or obscured, such that the remaining information does not reasonably identify an individual. This includes, but is not limited to, name, date of birth, demographic information, location information and school identity.

"Directory Information" shall have the meaning set forth under FERPA cited as 20 U.S.C. 1232 g(a)(5)(A).

"Education Record" shall have the meaning set forth under FERPA cited as 20 U.S.C. 1232 g(a)(4).

"**Indirect Identifiers**" means any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty.

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

"Personally Identifiable Information" or "PII" means data, including Indirect Identifiers, that can be used to identify or contact a particular individual, or other data which can be reasonably linked to that data or to that individual's specific computer or device. Student PII includes, without limitation, those items set forth in the definition of PII under FERPA. When anonymous or non-personal information is directly or indirectly linked with Personally Identifiable Information, the linked non-personal information is also treated as personal information. Persistent identifiers that are not anonymized, De-Identified or aggregated are personal information.

"Program Communications" shall mean 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 (for example new features or content, including using for at home learning opportunities), and information about special or additional programs (e.g. Beyond School) offered through the Services or KidRewards website or application.

"Sell" consistent with the Student Privacy Pledge, does not include or apply to a purchase, merger or other type of acquisition of a company by another entity, provided that the company or successor entity continues to treat the Personally Identifiable Information contained in Student Data in a manner consistent with this DPA with respect to the previously acquired Personally Identifiable Information contained in Student Data. Sell also does not include sharing, transferring or disclosing Student Data with a Service Provider that is necessary to perform a business purpose (such as detecting security incidents, debugging and repairing, analytics, storage or other processing activities) provided that the Service Provider does not Sell the Student Data except as necessary to perform the business purpose. Provider is also not "selling" personal information (i) if a user directs Provider to intentionally disclose Student Data or uses KidRewards to intentionally interact with a third party, provided that such third party also does not Sell the Student Data; or (ii) if a parent or other user (with parent consent) purchases Student Data (e.g. enhanced classroom reports or photos).

"Service Provider" 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, and who has access to PII.

"School Official" means for the purposes of this DPA and pursuant to FERPA (34 CFR 99.31 (B)), a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of Education records; and (3) Is subject to FERPA (34 CFR 99.33(a)) governing the use and re-disclosure of personally identifiable information from Education Records.

"Student Data" means any Personally Identifiable Information, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, for a school purpose, that is descriptive of the student including, but not limited to, information in the student's Educational Record or email, first and last name, home address, telephone number, email address, or other information allowing online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information text messages, documents, student identifies, search activity, photos, voice recordings or geolocation information. To the extent U.S. law applies, Student Data may include Education Records. 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 include De-Identified Data or information that has been anonymized, or anonymous usage data regarding a student's use of Provider's Services.

"Student Generated Content" means materials or content created by a student including content created at the direction of the LEA personnel or during classroom use of the Services, such as, 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. "Student Generated Content" does not include student responses to a standardized assessment where student possession and control would jeopardize the validity and reliability of that assessment.

"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 website, online service or mobile application by such student or the retention of such student's online activities or requests over time and across non-affiliate websites for the purpose of targeting subsequent advertising. This does not include advertising to a student based on the content of a web page, search query or a user's contemporaneous behavior on the website or a response to a student's response or request for information or feedback, both of which are permitted.

EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF STUDENT DATA

LEA directs KidRewards to dispose of Student Data obtained by Provider pursuant to the terms of the DPA between LEA and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

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

[Insert categories of data here]

__ Disposition is Complete. Disposition extends to all categories of Student Data.

2. Nature of Disposition

__ Disposition shall be by destruction or deletion of Student Data, including De-Identification of Student Data as set forth in Section 4.6 ("Disposition of Data").

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

[Insert or attach special instructions]

3. Timing of Disposition

Student Data shall be disposed of by the following date:

__ As soon as commercially practicable

___By *[Insert Date]*

4. Signature

_____
Authorized Representative of LEA

_____
Date

5. Verification of Disposition of Data

_____
Authorized Representative of Company

_____
Date

EXHIBIT "E"

DATA SECURITY REQUIREMENTS

Please see our Security Whitepaper for details: https://www.kidrewards.org/security.html