Data Processing Agreement (USA)

Effective Date: August 25, 2023

This Data Processing Agreement ("DPA"), forms part of the subscription license agreement (the "License Agreement") between Respondus, Inc. ("Respondus") and Licensee (as defined below) for Licensee's access to and use of Respondus Service(s) (as defined below) and related technical support to Licensee. This DPA reflects the parties' agreement with respect to the processing and security of Personal Data from or about Licensee's students and other persons ("Students") under the License Agreement ("Licensee Data").

Respondus reserves the right to modify this DPA at any time. If Respondus modifies the DPA, it will post the new version in the Respondus Privacy Center. Respondus may include a notice on the home page or any other place deemed appropriate. If these are material changes, Respondus may notify Licensee via an email address that Licensee provided.

1. Definitions and interpretation

1.1. In this DPA, the following terms shall have the following meanings:

"Applicable Data Protection Law" means FERPA, US state legislation and any applicable laws, regulations and other legal requirements relating to (a) privacy and data security; and (b) the use, collection, retention, storage, security, disclosure, transfer, disposal and other processing of Personal Data.

"Controller," "Processor," "Data Subject," "Personal Data," and "Processing" (and **"Process")** shall have the meanings given in Applicable Data Protection Law.

"Documentation" means the License Agreement and/or Terms of Use and the User Guide for each Service as provided by Respondus to each Licensee and found at the Respondus website, https://respondus.com/

"EU-U.S. Data Privacy Framework" means the EU-U.S. Data Privacy Framework self-certification program operated by the U.S. Department of Commerce and approved by the European Commission pursuant to Decision C (2023) 4745 of July 10, 2023.

"Licensee" means the entity that entered into the License Agreement with Respondus for the Respondus Service.

"Service" or "Respondus Service" means the services provided pursuant to a subscription to one or more of the following Respondus products: LockDown Browser, Respondus Monitor and StudyMate Campus. A further description of each Service can be found in the Documentation.

"Subprocessor" means any third-party Processors engaged directly by Respondus to assist with Respondus' processing of Licensee Data.

"Security Incident" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

“Non-Licensee Controlled Data” means usage and operations data in connection with the Licensee’s use of the Respondus Services, not including End User use, but including Licensee Administrator login information, query logs, and metadata (ie object definitions and properties). This definition does not include de-identified or anonymous usage data regarding a Student’s use of Respondus Services.

1.2. Capitalized terms used but not defined in this DPA shall have the meanings given in the Agreement or in the Applicable Data Protection Law.

2. Data Protection

2.1. Relationship of the parties. The parties acknowledge and agree that under the License Agreement, Licensee is the Data Controller and Respondus is a Data Processor, appointed to process the Licensee Data on Licensee's behalf. Each party shall comply with the obligations that apply to it under Applicable Data Protection Law.

2.2. Purpose and background. Licensee uses the Services to monitor certain activities of its Students and in doing so it gathers the Licensee Data regarding its Students. The parties acknowledge that Licensee Data comprises Personal Data under the Applicable Data Protection Law. Respondus stores and processes some of the Licensee Data on its servers as part of the Services. The Licensee maintains ownership and controls all access to the Licensee Data in its account, and Respondus has access by virtue of maintaining the servers and providing the software for the Services. The nature of the processing and the type of data processed is described in Documentation and the duration of the processing is the term specified in the License Agreement. Respondus agrees that it will not access any Licensee Data except (i) as necessary for the operation of the Services, as described in the Documentation and (ii) as expressly permitted by the Licensee (together, the "Permitted Purpose"), except where otherwise required by any law applicable to Licensee. Respondus may, however, de-identify Licensee Data ("De-Identified Data") and may process De-Identified Data to maintain and improve the Services.

2.3. International transfers. Licensee acknowledges that Respondus' maintains servers located in the United States of America, and that processing of Licensee data takes place therein. Licensee further acknowledges that because Respondus' servers are located outside of the European Economic Area ("EEA") that the Licensee Data will be transferred outside of the EEA for processing as part of the Services. Licensee is responsible for informing Students impacted from such transfers out of the EEA and obtaining their consent from all Students for these transfers. To facilitate such consent, the parties shall take such measures as are necessary to ensure the transfer is in compliance with Applicable Data Protection Law. Such measures may include (without limitation) transferring the Licensee Data to a recipient that has executed standard contractual clauses adopted or approved by the European Commission.

2.4. Security. Respondus shall implement appropriate technical and organizational measures to protect the Licensee Data from unlawful processing and/or a Security Incident. Such measures shall have regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the nature, likelihood and severity of the risk to the rights and freedoms of natural persons. Such measures shall include, as appropriate:

(a) the pseudonymization or encryption of personal data;

(b) ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

2.5 EU-U.S. Data Privacy Framework, UK Extension, Swiss-U.S. Data Privacy Framework. Respondus will provide at least the same level of protection for the Licensee Data as is required under the EU-U.S Data Privacy Framework, the UK Extension to the EU-U.S. DPF and the Swiss-U.S. Data Privacy Framework, and shall promptly notify Licensee if it makes a determination that it can no longer provide this level of protection. In such event, or if Licensee otherwise reasonably believes that Respondus is not protecting the Licensee Data as required under the EU-U.S Data Privacy Framework, the UK Extension to the EU-U.S. DPF and the Swiss-U.S. Data Privacy Framework, Licensee may either: (a) instruct Respondus to take reasonable and appropriate steps to stop and remediate any unauthorized processing, in which event Respondus shall promptly cooperate with Licensee in good faith to identify, agree and implement such steps; or (b) terminate this DPA and the Agreement without penalty by giving notice to Respondus.

2.6 Respondus Personnel. Respondus shall ensure that any person that it authorizes to process the Licensee Data (including Respondus' staff, agents and subcontractors) (an "Authorized Person") shall be subject to a legally-binding duty of confidentiality. Respondus shall ensure that all Authorized Persons maintain the security of all Licensee Data and process the Licensee Data only as necessary for the Permitted Purpose.

2.7. Subprocessing. Licensee acknowledges that Respondus' servers that house the Services are controlled and operated by a third-party hosting provider and that such provider is a Subprocessor under the Applicable Data Protection Law. Licensee hereby consents to Respondus appointing Amazon Web Services ("AWS") as such a Subprocessor. Respondus may change or appoint additional Subprocessors by posting notice (including the identity and details of the processing to be performed) at the following URL: web.respondus.com/privacy/subprocessors/. Respondus shall impose data protection terms on any Subprocessor that are consistent with the terms of this DPA and the Applicable Data Protection Laws. Respondus remains fully liable for any breach of this DPA by an act, error or omission of its Subprocessor. If Licensee declines to consent to Respondus' appointment of a Subprocessor, Licensee may elect to suspend or terminate the License Agreement and this DPA, subject to payment of all fees due for services rendered.

3. Cooperation and data subjects' rights

3.1. Assistance. During the Term, Respondus shall provide reasonable assistance to Licensee to respond to (a) any request from a data subject to exercise any of its rights under Applicable Data Protection Law (including its rights of access, correction, objection, erasure and data portability, as applicable); and (b) any other correspondence, enquiry or complaint received from a data subject, regulator or other third-party in connection with the processing of the Licensee Data as required under the Applicable Data Protection Law.

3.2. Direct Requests. If Respondus receives any requests from a data subject related to Licensee Data, Respondus shall (i) advise the data subject to provide such request directly to the Licensee, and Licensee shall be responsible for responding to such request, and (ii) notify the Licensee, if known, of the request. Respondus shall comply with reasonable requests by Licensee to assist with Licensee's response to such a data subject request.

3.3. Data Protection Impact Assessment. Upon Licensee's written request and to the extent that Licensee does not otherwise have access to the relevant information and the information is available to Respondus, Respondus shall provide Licensee with reasonable assistance (at Licensee's cost) needed to fulfill the Licensee's obligations under Applicable Data Protection Law to carry out a data protection impact assessment related to Licensee's use of the Service. To the extent necessary, Respondus shall provide reasonable assistance to the Licensee in the consultation with its relevant data protection authority.

4. Security incidents

If Respondus becomes aware of a confirmed Security Incident that involves Licensee Data, Respondus will: (a) notify Licensee of the Security Incident without undue delay; (b) take appropriate steps to identify the cause of the Security Incident, minimize harm and secure the Licensee Data; and (c) provide Licensee with information as may be reasonably necessary to assist Licensee with its notification and reporting responsibilities. Respondus will not evaluate the contents of the Licensee Data to identify any specific reporting or other legal obligations that are applicable to the Licensee. Any and all regulatory and/or data subject reporting obligations related to the Security Incident are the responsibility of the Licensee. Respondus' notification of or response to a Security Incident under this DPA will not be construed as an acknowledgement by Respondus of any liability or fault with respect to the Security Incident.

5. Data Retention and Deletion of Licensee Data.

At all times during the Term, Licensee will have the ability to access the Licensee Data. Respondus will retain Licensee Data for the period of time described in the Documentation. If the subscription is terminated, Respondus will disable Licensee's access to the Licensee Data. Access can be restored within the retention period by reinstating a valid subscription. The Licensee Data will be deleted at the end of the retention period, except as follows:

This requirement shall not apply: (a) to the extent that Respondus is required by law to retain some or all of the Licensee Data, in which event Respondus shall isolate and protect the Licensee Data from any further processing except to the extent required by such law or (b) to any data stored on back-ups, provided that such data will be destroyed in accordance with Respondus' standard retention policies for back-up data.

Upon termination of the Licensee's elected data retention period, or upon request of the Licensee, Respondus shall delete all Personal Data processed on behalf of the Licensee, unless a further period of time is provided for the storage of Personal Data under a provision of Applicable Data Protection Law. Upon request, Respondus shall provide a written statement confirming the deletion of the Licensee Data along with the deletion of all existing copies of the Licensee Data, within and no later than 7 (seven) days from the deletion of the Licensee Data.

6. Audit.

Respondus shall maintain complete and accurate records and information to demonstrate its compliance with this DPA. These records include HECVAT, SOC 2, and TXRAMP. The indices of internal policies can be made available for audit by Licensee or any regulatory authority having jurisdiction. In particular, Respondus shall respond to written audit questions submitted by Licensee related to Respondus' processing and protection of Licensee Data. Licensee shall not exercise this right more than once per year. Respondus will immediately inform Licensee if it believes that any Licensee instruction violates the Applicable Data Protection Law.

7. Legal Disclosures.

If Respondus is required by any legal or regulatory proceeding or requirement, to disclose any Licensee Data, it will provide Licensee with notice and a copy of the demand as soon as practicable, unless it is legally prohibited from doing so.

8. Jurisdiction Specific Items.

CCPA CONTRACT CLAUSES FOR SERVICE PROVIDERS

8.1 Definitions. The following definitions and rules of interpretation apply in this Agreement:

8.1.1. The definition of “Applicable Data Protection Law” includes the CCPA. CCPA means the California Consumer Privacy Act of 2018, as amended (Cal. Civ. Code §§ 1798.100 to 1798.199.95), the CCPA Regulations (Cal. Code Regs. tit. 11, §§ 7000 to 7102), and any related regulations or guidance provided by the California Attorney General.

8.1.2. Terms defined in the CCPA, including, without limitation, “Business”, “Service Provider”, “Consumer”, and “Personal Information”, carry the same meaning in this Agreement unless otherwise defined herein.

8.1.3. The definitions of: “controller” includes “Business”; “processor” includes “Service Provider”; “data subject” includes “Consumer”; “personal data” includes “Personal Information”; in each case defined under the CCPA and carry the same meaning in this Agreement.

8.2 Respondus acknowledges and agrees to comply with the applicable terms of the California Consumer Privacy Act of 2018 as amended (Cal. Civ. Code §§ 1798.100 - 1798.199) including applicable regulatory or other guidance ("CCPA").

8.3 With respect to Licensee Data, the parties hereby agree that Respondus is a "service provider" under the CCPA.

8.4 As a service provider for the Licensee, Respondus agrees:

8.4.1. Respondus will not collect, retain, use, or disclose personal information it accesses, receives, or creates pursuant to the Agreement ("Licensee Data") for any purpose other than for the purposes set out in the Agreement and as permitted under the CCPA. Respondus acknowledges that Licensee is disclosing or making available Licensee Data to Respondus only for the limited and specified purposes and services set for in the Agreement (“Services” or “Respondus Services”).

8.4.2. Respondus will not sell or share Licensee Data.

8.4.3. Respondus will not collect, retain, use, or disclose Licensee Data for any commercial purpose other than the Services, nor for any purposes outside of its direct business relationship with the Licensee, unless expressly permitted under the CCPA. Respondus will not combine or update Licensee Data with personal information that Respondus receives from or on behalf of another person, or that Respondus collects from its own interactions with the Student, unless permitted under the CCPA and the Licensee.

8.4.4. Respondus shall comply with all applicable sections of the CCPA with respect to Licensee Data and shall provide the level of privacy protection to Licensee Data as is required of businesses thereunder. Such compliance may include, without limitation, implementing reasonable security procedures and practices, appropriate to the nature of the Licensee Data, to protect that information from unauthorized or illegal access, destruction, use, modification, or disclosure in accordance with Cal. Civ. Code § 1798.81.5

8.4.5. Respondus will promptly notify the Licensee if it determines that it can no longer meet its obligations under applicable provisions of the CCPA.

8.4.6. Respondus shall comply with the Licensee's right to take reasonable and appropriate steps to ensure that Respondus uses Licensee Data in a manner consistent with the Licensee's obligations under the CCPA. These steps may include, without limitation, automated scans of Respondus' information systems, and regular internal or third-party assessments, audits, or other technical and operational testing at least once every 12 months.

8.4.7. Respondus shall comply with the Licensee's right, upon notice, to take reasonable and appropriate steps to stop and remediate use of Licensee Data that is unauthorized under the CCPA, including, without limitation, requiring Respondus to provide documentation verifying that it no longer retains or uses Licensee Data where Licensee submitted to Respondus a valid request to delete.

8.4.8. In the event Respondus is legally required to disclose personal information for a purpose unrelated to the Services, Respondus will, unless legally prohibited, inform the Licensee of the legal requirement and give it reasonable opportunity to object to or challenge the disclosure.

8.4.9. If the Services require the collection of Licensee Data by Respondus directly from Students on the Licensee's behalf, the Licensee will, at or before authorizing Respondus to collect such Licensee Data, provide those Students a CCPA-compliant notice at collection in a manner and format consistent with the CCPA. Licensee will notify Students and Respondus if any material modifications or alterations are made to such notices.

8.4.10. Respondus shall reasonably cooperate with the Licensee to comply with Student requests made pursuant to the CCPA. In the event Respondus receives requests directly from Students, Respondus will promptly inform Licensee of such requests, but not later than five (5) days following receipt and reasonably cooperate with Licensee in responding to them.

8.4.11. If Respondus subcontracts with another person in connection with the Services, such subcontractor used must qualify as a service provider under the CCPA and Respondus cannot make any disclosures to the subcontractor that the CCPA would treat as a sale.

8.4.12. For each subcontractor used, Respondus shall:

8.4.12.1. notify the Licensee of the engagement;

8.4.12.2. have a written contract with such person that complies with CCPA, including with respect to such person's Service Provider's or contractors.

8.4.13. Notwithstanding anything in the Agreement or any Order Form entered in connection therewith, the parties acknowledge and agree that Respondus' access to Licensee Data does not constitute part of the consideration exchanged by the parties in respect of the Agreement.

8.4.14. To the extent that any Non-Licensee Controlled Data (as defined in the Agreement) is considered Personal Data, Respondus is the Business with respect to such data and will Process such data in accordance with its Privacy Policy, which can be found at https://web.respondus.com/privacy-non-product/

APPENDIX A

Personal Information Processing Purposes and Details

Contracted Business Purposes: "Service" or "Respondus Service", as defined in the USA DPA

Service Provider Category: Service Provider

Personal Information Categories:

- This Agreement involves the following types of *Categories* of data subjects:
    - Students enrolled in the Licensee's institution or program
    - Employees of the Licensee
- This Agreement involves the processing of the following types of *Personal Information and Sensitive Personal* of data subjects as defined and classified in CCPA Cal. Civ. Code § 1798.140(o).

We process the personal information and sensitive personal information categories listed in the tables below under this Agreement.

Sensitive personal information is a subtype of personal information consisting of specific information categories. While we collect information that could be deemed as falling within the sensitive personal information categories listed in the table below, the CCPA does not treat this information as sensitive because we do not collect or use it to infer characteristics about a person.

Personal Information Category	Examples
Identifiers.	This includes real name, alias (user name), postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, driver's license number. (*email address is optional - may be provided by students when obtaining technical support or making general inquiries*) (*driver's license or state ID card student ID card is also optional, depending on Licensee's operational requirement*)
California Customer Records personal information.	This includes a name, signature, address, telephone number, driver's license or state identification card number or student identification card number, employment position.

	Some personal information included in this category may overlap with other categories. (*driver's license or state ID card student ID card is optional, depending on Licensee's operational requirement*)
Commercial information.	This includes records of services purchased.
Internet or other similar network activity.	This includes information on a consumer's interaction with Respondus website, application, or advertisement.
Non-public education information.	This includes education records directly related to a student maintained by an educational institution or party acting on its behalf, such as grades, class lists, student identification codes. Also includes education data. (*education data includes proctoring analysis: Analysis data from exam session, such as duration of exam or time spent per question, or flags indicating possible exam rule violations*) (*education data also includes photos, video and audio; video/audio recording of the examinee; a photo image of the examinee is optional, depends on Licensee's operational requirements*) (*education data such as grades, class lists, and student educations codes are processed but not stored*)

Sensitive Personal Information Category	Examples
Government identifiers.	This includes driver's license, or state identification card or student identification card (*driver's license or state ID card student ID card is optional, depending on Licensee's operational requirement*)