Data Privacy and Security Agreement

Prince George's County Public Schools and _____.

This 1EdTech Data Privacy and Security Agreement ("DPSA") is entered into by and between the institution entity defined in the signature block below ("Institution") and the third-party provider listed in the signature block below ("Vendor") (individually a "Party", together the "Parties"). This DPSA is effective as of the last signature date below (the "Effective Date"). In the event of a conflict between this DPSA or any other writing between the Parties, this DPSA shall control with respect to the subject matter herein.

The Parties agree as follows.

1. Definitions.

- **"Affiliate(s)"** means any entity, subsidiary, parent, or other organization that shares at least 50% ownership with a party.
- **"Institution Data"** means any proprietary or confidential data provided by Institution to Vendor or created by Vendor on behalf of Institution in the provision of the Services. Institution Data includes without limitation Educational Records and Personally Identifiable Information (as defined below) and includes confidential information as defined in the Service Agreement. Institution Data does not include Services use data used by the Vendor for internal operations.
- **"Data Breach"** means an actual breach of security, privacy, or Data Protection Laws leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Institution Data created, transmitted, stored, or otherwise Processed by Vendor.
- **"Data Protection Law(s)"** means the laws and regulations that are applicable to the Processing of Personally Identifiable Information or Institution Data Processed by Vendor under this DPSA, including without limitation, FERPA (defined below), the Children's Online Privacy and Protection Act ("COPPA") at 15 U.S.C. § 6501-6505 and 16 CFR Part 213, the Protection of Pupil Rights Amendment at 34 CFR Part 90 ("PPRA"), the Children's Internet Protection Act at 20 U.S.C. § 9132 and 254 ("CIPA") and any applicable federal and state laws governing the protection of Personally Identifiable Information.
- **"De-identified Data"** means data and information where all Personally Identifiable Information has been removed or obscured such that the remaining data and information does not reasonably identify a specific individual, including

but not limited to, any information that, alone or in combination is linkable to a specific individual. Provided, however, data sets with less than twenty (20) individuals are not considered “de-identified”.

- **“Disclosure”** means to permit access to or the release, transfer or other communication of Personally Identifiable Information or Education Record by any means, including oral, written, or electronic means, to any unauthorized third-party.
- **“Educational Records”** means records, files, documents, and other materials directly related to a student including Student Generated Content and created or maintained by the Institution, or by a person acting on behalf of the Institution.
- **“FERPA”** means the Family Educational Rights and Privacy Act at 20 U.S.C. § 1232g and regulations at 34 CFR Part 99.
- **“Personally Identifiable Information”** or **“PII”** means any information relating to an identified or reasonably identifiable individual. This includes indirect information or identifiers; or other information that, alone or in combination, is linked or linkable to a specific person that would allow a reasonable person, who does not have personal knowledge of the relevant circumstances, to identify an individual with reasonable certainty.
- **“Processing”** means any operation or set of operations which is performed upon Personally Identifiable Information whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, Disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction **(“Process”, “Processes”** and **“Processed”** shall have the same meaning).
- **“School Official”** means is an entity that, (a) performs an institutional service or function for which the Institution would otherwise use employees; (b) is under the direct control of the Institution with respect to the use and maintenance of Student Data including Education Records; and (c) Is subject to 34 CFR § 99.33(a) governing the use and re-Disclosure of Personally Identifiable Information from Education Records.
- **“Service Agreement”** means the current contract for Services between the Institution and Vendor.
- **“Services”** means the software, services, goods, or other materials described in the Service Agreement and includes the underlying infrastructure, hosting, and networks.
- **“Student Generated-Content”** means any content created by a student through their use of the Services, including, but not limited to, essays, research papers, portfolios, creative writing, music or other audio files, or photographs, except

"student-generated content" does not include student responses to a standardized assessment, or responses to other assessments.

- **"Subprocessor(s)"** means any third-party engaged by the Vendor that Processes Personally Identifiable Information or Education Records on behalf of the Vendor.

2. Term; Termination.

2.1. Term. This DPSA shall commence on the Effective Data and shall continue for the term of the Service Agreement, unless terminated earlier in accordance with this DPSA.

2.2. Termination.

(a) During the term of the Service Agreement, this DPSA may be terminated by either Party upon thirty (30) days prior written notice to the other Party. In the event of such termination, Vendor shall stop Processing Institution Data and dispose of Institution Data as described in Section 4.9.

(b) In the event of an incurable breach of this DPSA by the Vendor, Institution may terminate this DPSA immediately. In the event of such termination, Vendor shall stop Processing Institution Data and dispose of Institution Data as described in Section 4.9.

(c) This DPSA shall automatically terminate upon the same date as the Service Agreement unless otherwise agreed to by the Parties. In the event of such termination, Vendor shall stop Processing Institution Data and dispose of Institution Data as described in Section 4.9.

3. Data Use, Ownership, and Obligations.

3.1. Data Ownership. As between Institution and Vendor, Institution owns and controls all Institution Data provided to; or generated by Vendor under this DPSA and the Service Agreement. All rights and intellectual property in and to Institution Data shall remain the exclusive property of the Institution. Any modifications, copies, additions to or any portion of the Institution Data are subject to the provisions of this DPSA.

3.2. Data Location. Vendor will store or host all Educational Records and Personally Identifiable Information in the continental USA.

3.3. FERPA. To the extent that the Institution is subject to FERPA, the Parties agree that Vendor operates as a School Official under FERPA and has a legitimate educational interest in Personally Identifiable Information from Education Records received from the Institution pursuant to this DPSA. For purposes of the Agreement and this DPA, Vendor: (a) provides a service or function for which the

Institution would otherwise use its' employees; (b) is under the direct control of the Institution with respect to the use and maintenance of Education Records; and (c) is subject to the requirements of FERPA governing the use and re-Disclosure of Personally Identifiable Information from the Education Records received from Institution.

3.4. **Separate Account.** As required and defined by applicable Data Protection Laws, if Student Generated Content is created, stored, or maintained by Vendor or the Services, Vendor shall, at the request of the Institution, transfer or provide a mechanism for the Institution to transfer such Student Generated Content to a separate account created by the student or parent.

3.5. **De-Identified Data.** De-Identified data may be used by Vendor for those purposes permitted under FERPA and the following purposes: (a) assisting the Institution or other governmental agencies in conducting research and other studies; research and development of the Vendor's educational sites, services, or applications, and (b) to demonstrate the effectiveness of the Services; and for adaptive learning purpose and for customized student learning. Vendor's use of De-Identified Data shall survive termination of this DPA or any request by Institution to return or destroy Student Data. Vendor agrees not to attempt to re-identify De-Identified Data, and not to transfer De- Identified Student Data to any third party unless that third party agrees in writing not to attempt re-identification.

3.6. **Data Schedule.** The Vendor shall complete Exhibit A to describe the Institution Data elements Processed by the Services. The Vendor agrees to update Exhibit A as necessary when Institution Data elements are added or removed.

4. Vendor Obligations.

4.1. **Authorized Use.** Vendor shall only use Institution Data as provided in this DPSA and the Service Agreement to provide the Services. Except as expressly permitted herein, Vendor shall not disclose Institution Data to any third party without the prior written consent of Institution. Vendor may only share Institution Data with its Affiliates to provide the Services under the Agreement and any such access shall be on a need- to-know basis.

4.2. **Compliance with Data Protection Laws.** In its provision of the Services, Vendor agrees to comply with all Data Protection Laws applicable to its Processing of Institution Data.

4.3. **Advertising.** Vendor shall not sell, transfer, share, or otherwise disclose Personally Identifiable Information, Education Records, unique identifiers, or any Institution Data to targeted advertising providers or develop a profile of a student or parent or guardian for the purpose of advertising. Vendor will not use Institution Data for its own advertising or for third-party advertising. This does not prohibit Vendor from using Institution Data to provide adaptive learning services, customized student learning services, making product recommendations to

Institution employees, and notify account holders of updates about the Services or new features of the Services.

4.4. Vendor Personnel. Vendor shall ensure that its employees, Subprocessors, subcontractors, and agents (collectively **"Personnel"**) involved in the Processing of Personally Identifiable Information or Education Records are subject to either contractual or statutory obligations of confidentiality, and that access is strictly limited to those Personnel who require access to perform the Services. Vendor shall ensure that its Personnel are informed of the confidential nature of the Institution Data and have received appropriate training on their responsibilities and applicable Data Protection Laws. As required by Data Protection Laws or Institution policy, Vendor shall ensure that its Personnel have gone through appropriate background checks prior to accessing Personally Identifiable Information or Education Records.

4.5. Security and Privacy.

(a) Security and Privacy Program. Vendor shall implement and maintain a security and privacy program that includes appropriate physical, administrative, technical, and operational controls to protect the confidentiality, integrity, privacy, and availability of Institution Data Processed by Vendor aligned with an industry standard framework, for example such as the NIST Cybersecurity Framework, AICPA SOC 2 Type 2, ISO/IEC 27001, or other recognized industry standards. Vendor shall describe its security standards in Exhibit A. These measures shall include protection against unauthorized or unlawful access, processing, loss, alteration, damage of Institution's Personally Identifiable Information. Vendor shall regularly monitor its compliance with its program and not materially decrease its privacy and security controls during the term of this DPSA.

(b) Incident Response Plan. Vendor shall implement, maintain, and regularly test an incident response plan consistent with industry standard practices and Data Protection Laws. This incident response plan shall include processes for responding to a Data Breach, breach of the security, privacy, or unauthorized acquisition or use of Institution Data or any portion thereof, including PII and agrees to provide Institution with a summary of said written incident response plan so long as a valid non-disclosure agreement in place between the parties.

4.6. Data Breach. In the event of a Data Breach, Vendor shall promptly, but in no more than seventy-two (72) hours, notify Institution of any such Data Breach unless prohibited by an applicable law enforcement authority. Vendor shall provide such notification to Institution's Security Contact as described in Section 7.5 or other contact as provided by Institution. In such notification Vendor shall provide the following information, to the extent such information becomes available to Vendor; (a) a general description of the Data Breach; (b) the categories and approximate number of records or individuals affected by the Data Breach; (c) actions taken by Vendor to remediate the Data Breach; and (d)

Vendor shall (i) take reasonable steps to mitigate the effects and minimize any damage resulting from the Data Breach; (ii) cooperate with Institution's reasonable requests for assistance in remediating a Data Breach; and (iii) maintain records of information related to the Data Breach. If such information is not available within the timeframe specified, the Vendor shall include an estimated timeline to provide a complete detail of the above aspects.

4.7. Audits. No more than once every twelve (12) months Institution may audit Vendor's compliance with this DPSA and applicable Data Protection Laws for the purpose of meeting its obligations under Data Protection Laws or Institution's policies. Institution shall provide at least thirty (30) days written notice to the Vendor of such an audit.

(a) In lieu of an Institution audit, Vendor agrees to conduct an annual security and privacy audit of its Services and program. Upon receipt of a written request and execution of an appropriate confidentiality agreement, Vendor will provide copies of its most recent audit summary or bridge letter to Institution. Vendor agrees to have a third-party conducted penetration test, dated within the last twelve (12) months, with all high and above findings remediated.

(b) In the event of a Data Breach, or inquiry by any governmental agency, Institution (or the applicable governmental agency) may perform an audit of Vendor upon written notice to Vendor. Institution shall send any such audit request to the Security Contact identified in Section 7.5 (Notice). In the event that Institution engages a third party to perform the audit, such third party shall execute a non-disclosure agreement with Vendor. Institution agrees to promptly notify the Vendor of any non-compliance discovered during such an audit.

(c) The Vendor agrees in good faith to remediate any critical or high security findings, or known exploitable findings identified by the Institution.

4.8. Subprocessors. Institution agrees that Vendor may use Subprocessors in connection with the provision of the Services and permit Subprocessors to Process Institution Data, provided that:

(a) Vendor shall ensure that obligations not materially less protective than those set out in this DPSA, and applicable Data Protection Laws are imposed on its Subprocessors;

(b) Vendor shall be responsible for the acts and omissions of its Subprocessors if and to the same extent Vendor would be liable if performing the services of each Subprocessor directly;

(c) Vendor shall provide Institution of a list of its current Subprocessors in Exhibit B or by providing a link to a website where information about its list of Subprocessors are kept up to date; and

(d) Vendor shall inform the Institution of any changes or additions to its Subprocessors at least thirty (30) days prior to such addition or change.

4.9. Deletion and Return of Institution Data.

(a) Vendor shall (and procure that its Subprocessors shall) securely delete Institution Data stored in the Services (i) within ninety (90) days after termination of this DSPA; or (ii) within thirty (30) days upon written request from Institution. Upon written request from Institution, Vendor shall provide written certification of such deletion substantially in the form of Exhibit C. Until such deletion occurs, the Vendor will ensure compliance with this DPSA.

(b) Vendor shall provide functionality for Institution to download Institution Data from the Services, to the extent possible provided by the Services. If the Services do not provide a download functionality, the Vendor shall return to Institution all Institution Data in the Services in an industry standard format within ninety (90) days after termination of this DPSA.

(c) If Vendor believes that it cannot comply with the foregoing deletion requirement because applicable law requires the retention of such data then Vendor shall provide written notice to Institution within thirty (30) days of termination of this DPSA informing of such requirement and protect such data in accordance with this DPSA.

4.10. Law Enforcement Requests. If the Vendor receives a request for access to Institution Data from a legally authorized entity, the Vendor shall promptly notify Institution of such request unless prohibited from such notification by applicable law.

5. Institution Obligations.

5.1. Institution shall, in its use or receipt of the Services Process Institution Data in accordance with the Data Protection Laws. Institution will ensure that its instructions for the Processing comply with applicable Data Protection Laws. Institution shall have sole responsibility for the accuracy, quality, and legality of Institution Data, the means by which Institution obtained the Institution Data, and for fulfilling all requirements under Data Protection Laws necessary to make the Institution Data available to Vendor. Institution shall promptly notify Vendor of any known unauthorized access to the Services. Institution will assist Vendor in any efforts by Vendor to investigate and respond to any unauthorized access to the Services.

5.2. COPPA Obligations. Children under 13 may only use the Services with prior consent of a parent or an educational institution acting on behalf of the child's parent. Institution agrees that it has obtained such consent prior to permitting any child under 13 from accessing or using the Services.

6. Insurance.

In addition to any insurance requirements under the Service Agreement, Vendor shall secure and maintain at Vendor's sole expense the insurance coverages described Exhibit E.

7. Miscellaneous.

7.1. Severance. Should any provision of this DPSA be invalid or unenforceable, then the remainder of this DPSA shall remain valid and in force. The invalid or unenforceable provision shall be either amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or, if this is not possible, construed in a manner as if the invalid or unenforceable part had never been contained therein.

7.2. Entire Agreement. This DPSA and the Service Agreement constitutes the entire of agreement of the Parties with respect the subject matter hereof and supersedes any prior or contemporaneous representations, understandings, writings, or agreements by the Parties. This DPSA may only be amended by the Parties in writing.

7.3. Governing Law; Jurisdiction; Venue. This DSPA shall be governed by and construed in accordance with the laws of the state of Institution without regard to conflicts of laws principles. The Parties agree to submit to the jurisdiction of the state and federal courts located in the state of the Institution.

7.4. Assignment. Vendor may not assign its rights and obligations under this DPSA without the consent of the Institution which shall not be unreasonably withheld. Any such assignment without consent shall be considered null and void. Notwithstanding the foregoing, Vendor may assign its rights and obligations under this DPSA, in whole or part, in connection with the transfer or sale of all or substantially all of the assets or business of Vendor. This DPSA will be binding upon, incur to the benefit of, and be enforceable by the Parties and respective successors and permitted assigns.

7.5. Notices. Any notice required or permitted to be given under this DPSA shall be in writing and shall be addressed to the appropriate Party at the address specified below. Notices shall be deemed to have been given for all purposes (a) when delivered if sent by a reputable courier service, or (b) five (5) days after mailing, or (c) upon receipt when delivered by email provided that the recipient acknowledges such delivery.

Institution Legal Notice Representative	Institution Security Representative
Name:	**Name:**
Title: General Counsel	**Title:**
Address: 14201 School Lane, Upper Marlboro, MD 20772	**Address:** 14201 School Lane, Upper Marlboro, MD 20772
Phone: 301-952-6063	**Phone:** 301-952-6250
Email:	**Email:**

Vendor Legal Notice Representative	Vendor Security Representative
Name:	**Name:**
Title:	**Title:**
Address:	**Address:**
Phone:	**Phone:**
Email:	**Email:**

[Signatures to Follow]

Agreed and accepted.

	Prince George's County Public Schools
Vendor Name	**Institution Name**
	14201 School Lane
Address	**Address**
	Upper Marlboro, MD 20772
City/State/Zip	**City/State/Zip**
Signature	**Signature**
Name	**Name**
Title	**Title**
Date	**Date**

Exhibit A

(Part 1) - Schedule of Institution Data

(Part 2) - Vendor Security Standards

Exhibit A - Institution Data Schedule and Vendor Security Practices is a required component. It is provided as an editable document for your convenience. The finalized version will be incorporated into the fully executed DPSA PDF.

Access Exhibit A and the directions at:

https://bit.ly/PGCPS_DPSAExhibitA

This page will be replaced by the completed Exhibit A upon review

***Sensitive data field, SOC 2 or similar required**

Exhibit B - Subprocessor List

All currently approved subprocessors are listed below or attached. **All columns** must be addressed. If no subprocessors are used, select the checkbox below.

☐ **No subprocessors are used in the support or delivery of this product.**

Subprocessor Name	Subprocessor Address	Processing Activities	Institution Data Processed	Processing and/or Hosting Location

Exhibit C - Data Deletion Certificate Template

The undersigned hereby certifies that all copies of Institution Data collected, created, or processed by_____ on behalf of Prince George's County Public Schools have been securely deleted from Vendor's Services on _____.

By signing this certificate, Vendor confirms that all Institution Data, including copies, derivatives, subsets, manipulated files, system backups, temporary files, including non-electric media, held by Vendor, its employees, subcontractors, agents, and Subprocessors have been properly disposed in accordance with the Data Privacy and Security Agreement.

_____
Signature

_____
Name

_____
Title

Vendor Name: _____

Address: _____

Exhibit D - Institution Specific Requirements

- Vendor agrees that this DPA governs the relationship between Vendor and PGCPS with respect to Data Privacy and supersedes any Vendor Data Privacy policies.

- Vendor acknowledges and agrees that PGCPS is providing consent on behalf of students and parents for core educational functions only. This does not extend to sharing data with third parties for non-educational purposes.

- **3.6 Data Schedule**. The Vendor shall complete Exhibit A to describe the Institution Data elements Processed by the Services. The Vendor agrees to update Exhibit A as necessary when Institution Data elements are added or removed and will notify the Institution in writing within 30 days.

- **4.9 Deletion and Return of Institution Data.**

  (a) Vendor shall (and procure that its Subprocessors shall) securely delete Institution Data stored in the Services (i) within ninety (90) days after termination this DSPA; or (ii) within thirty (30) days upon written request from Institution. Vendor shall provide written certification of such deletion substantially in the form of Exhibit C, **within thirty (30) days of deletion**. Until such deletion occurs, the Vendor will ensure compliance with this DPSA.

  (b) Vendor shall provide functionality for Institution to download Institution Data from the Services, to the extent possible provided by the Services. If the Services do not provide a download functionality, the Vendor shall return to Institution all Institution Data in the Services in one of the following formats csv, xlsx, XML, Microsoft Access within ninety (90) days after termination of this DPSA.

Exhibit E - Insurance Coverages

Insurance coverages shall be with an admitted carrier having at least an “A” BEST rating. The Vendor shall include the Institution as an additional insured and provide evidence of such coverages upon request by Institution.

Cyber liability coverage providing protection against (i) privacy breaches (liability arising from the loss or Disclosure of Institution Data); (ii) system breach; (iii) denial or loss of service; (iv) introduction, implantation, or spread of malicious software code; and (v) unauthorized access or use of computer systems with a limit of at least

$ **One Million Dollars ($1,000,000.00)** per occurrence.

Commercial general liability insurance covering bodily injury and property damage to third parties and including Products/Completed Operations and Blanket Contractual Liability, covering Vendor and its employees, at the following limits:

$ **One Million Dollars ($1,000,000.00)** per occurrence.

$ **Three Million Dollars ($3,000,000.00)** general aggregate.

Exhibit F - Data Privacy and Security Agreement Variations

Any variations to the DPSA agreed to between the Parties shall be listed below.

Section Number	Original Language	Revised Language

Section Number	Original Language	Revised Language