STUDENT DATA SHARING AGREEMENT:
Amendment to [VENDOR] Terms of Service
APPLICABLE TO ###### PUBLIC SCHOOL SYSTEM USERS/MEMBERS

This Amendment is an agreement between VENDOR ("VENDOR", or "Company") and the ###### Public School System ("####," "System," or "CLIENT") for term beginning on #####, 2017 and ending on June 30, 2018.

#####, as a Government entity, is required when entering into agreements with other parties to follow all applicable laws and regulations, including those related to data privacy and security; accessibility; and records retention. Accordingly, the Terms of Service (TOS) are hereby modified by this Amendment as they pertain to #####'s use of the Company's Site and/or Services.

A. ***Definition of "CLIENT Data"***: CLIENT Data include all Personally Identifiable Information (PII) and other non-public information. CLIENT Data include, but are not limited to, student data, metadata, and user content.

B. ***Data Collection and Use:*** VENDOR will collect and use CLIENT Data only for the purpose of fulfilling its duties and providing services under this Agreement, and for improving services under this Agreement.

   1. ***Specific Data Shared Under this Agreement***
       i.   Information associated with maintaining authentication between VENDOR and CLEINT, e.g. public/private keys, LTI secret, OATH keys.
       ii. Information associated with maintaining a user's profile, e.g. username, email address, first name, last name, source IP address, or cookies.
       iii. A user's status within the service, e.g. number of questions answered, time elapsed in lesson, student's score.

C. ***Education Records***: If VENDOR will have access to "education records" as defined under the Family Educational Rights and Privacy Act (FERPA) (34 CFR Part 99), the VENDOR acknowledges that for the purpose of this Agreement it will be designated as a 'school official' with 'legitimate educational interests' and will use the data only for the purpose of fulfilling its duties under this Agreement. VENDOR agrees to indemnify and hold harmless the Board of Education of #### School for any damages or costs, including reasonable attorney's fees, which arise out of any gross negligence or willful misconduct by VENDOR, its agents and employees concerning its FERPA obligations under this section.

D. ***Obligation of Confidentiality***: In performing services under this Agreement, VENDOR and CLIENT may be exposed to and will be required to use certain "Confidential Information", as defined below. VENDOR and CLIENT along with their employees, agents or representatives will not, use, directly or indirectly, such Confidential Information for purposes other than the purposes outlined in this Agreement.

E. ***Definition of Confidential Information:*** "Confidential Information" means information, not generally known, and proprietary to the VENDOR or CLIENT or to a third party for whom the VENDOR or CLIENT is performing work, including, without limitation, information concerning any patents or trade secrets, confidential or secret designs,

processes, formulae, source codes, plans, devices or material, research and development, proprietary software, analysis, techniques, materials or designs (whether or not patented or patentable), directly or indirectly useful in any aspect of the business of the VENDOR or CLIENT. Confidential Information includes all information which VENDOR or CLIENT acquires or becomes acquainted with during the period of this Agreement, whether developed by VENDOR, CLIENT or others, which VENDOR or CLIENT has a reasonable basis to believe to be Confidential, such as data that is personally identifiable to an individual student and information within the definition of "Education Record." The parties agree that the following will be treated as "Confidential Information": (i) all database information ("Data") provided by or on behalf of CLIENT to VENDOR; (ii) all information provided by VENDOR to CLIENT pertaining to the Services; (iii) all information which is labeled as such in writing and prominently marked as "Confidential," "Proprietary" or words of similar meaning by either party; or (iv) business information of a party which a reasonable person would understand under the circumstances to be confidential.

F. ***Maintenance of Confidentiality:*** Any Confidential Information acquired or received by either party (the "Recipient") in the course of this Agreement will not be disclosed or transferred to any person or entity other than to employees of a party and, as to VENDOR, for the purpose of performing its obligations under this Agreement. Confidential Information received under this Agreement will be treated with the same degree of care and security as each party uses with respect to its own Confidential Information, but not less than a reasonable degree of care. The parties agree to use Confidential Information only for the purpose of performance of this Agreement and to make no copies except as necessary for performance of this Agreement. Any such confidential information and copies thereof made by a party, or any representative of a party, shall be completely and promptly destroyed at the conclusion of contract performance subject to paragraph F.1 below.

    1. Upon termination or completion of the Services hereunder, upon request of CLIENT, VENDOR will delete the CLIENT's Confidential Information as housed in the VENDOR production database(s), provided that VENDOR may maintain archival copies for audit purposes and dispute resolution purposes and VENDOR may retain copies of Confidential Information on back-up media in which such Data is co-resident with other employment and income data. VENDOR shall remain under its contractual obligation of confidentiality and security to CLIENT and such obligations shall survive termination of the Agreement. This Section shall survive the termination of this Agreement.

G. ***Data De-Identification***: VENDOR may use de-identified Data for product development, research, or other internal purposes. De-identifiedData will have all direct and indirect personal identifiers removed. This includes, but is not limited to, name, ID numbers, date of birth, demographic information, location information, and school ID. Furthermore, VENDOR agrees not to attempt to re-identify de-identified Data.

H. ***Data Mining, Marketing and Advertising***: Except as indicated in Section G above, VENDOR is prohibited from mining CLIENT Data for any purposes other than those agreed to by the parties. **Data mining or scanning of user content for the**

purpose of advertising or marketing to students or their parents is prohibited. Any and all forms of advertisement, directed towards children, parents, guardians, or District Employees will be strictly prohibited unless allowed with express written consent of the District.

I. *Modification of Terms of Service:* VENDOR will not change how CLIENT Data are collected, used, or shared under the terms of this Agreement in any way without advance notice to the CLIENT. This Agreement is the entire agreement between the CLIENT (including all District end users) and the VENDOR. All other agreements or understandings, whether electronic, click-through, verbal or in writing, with District Employees or other End Users shall be null and void.

J. *Data Sharing:* VENDOR will not share CLIENT data, with or disclose it to any third party, except to affiliated subcontractors, agents, or third-party service providers of the VENDOR, without prior specific and informed written consent of the CLIENT, except as required by law.

K. *Data Storage:* CLIENT Data will not be stored outside of the United States without prior, specific and informed written consent from the CLIENT.

L. *Terms, Data Transfer, Survival and Destruction:* The CLIENT may immediately terminate the Agreement if the CLIENT determines the VENDOR has breached this Agreement. The Agreement will automatically terminate at the expiration date. However, the VENDOR's obligations shall survive termination of this Agreement until ALL CLIENT Data has been returned and/or securely removed or destroyed. VENDOR will ensure that all Data in its possession and in the possession of any subcontractors, or agents to which the VENDOR may have transferred Data, are destroyed.

M. *Rights and License in and to Data:* All goods, products, materials, documents, reports, writings, video images, photographs, papers and intellectual property of any nature including software or computer images prepared by the VENDOR (or subcontractors) for the CLIENT or from CLIENT-provided material will not be disclosed to any other person or entity and remains the property of the school system. All student-produced work remains the property of the school system or that eligible student. The VENDOR has a limited, nonexclusive license to the data described herein solely for the purpose of performing its obligations as outlined in the Agreement. This Agreement does not give VENDOR any rights, implied or otherwise, to Data, content, or intellectual property, except as expressly stated in the Agreement, including any right to sell or trade Data.

N. *Access:* Except as otherwise expressly prohibited by law, the VENDOR will immediately notify the CLIENT of any subpoenas, warrants, or other legal orders, demands or requests, including Audits, and governmental requests and demands, received by the VENDOR seeking CLIENT Data. If the CLIENT receives a similar request, the VENDOR will promptly supply the CLIENT with copies of records or information required by the CLIENT to respond.

O. *Security Controls and Risk Management:* VENDOR will store and process CLIENT

Data in accordance with industry best practices. This includes appropriate administrative, physical, and technical safeguards to: 1) ensure the security and confidentiality of PII and Confidential Information; 2) protect against any anticipated threats or hazards to the security or integrity of Confidential Information; 3) protect against unauthorized access to or use of Confidential Information that could result in substantial harm or inconvenience to any customer or to any client employee and/or student; and 4) dispose of PII and Confidential Information in a secure manner.

1. To comply with the safeguard obligations generally described above, VENDOR has (a) designated an employee to coordinate its information security program, (b) identified reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of CLIENT Information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assessed the sufficiency of any safeguards in place to control these risks, and (c) designed and implemented information safeguards to control the risks identified through the risk assessment, and regularly tests or otherwise monitors the effectiveness of safeguards' key controls, systems and procedures.

2. VENDOR will conduct periodic risk assessments and remediate any identified security vulnerabilities in a timely manner. VENDOR will also have a written incident response plan, to include prompt notification of ##### in the event of a security or privacy incident, as well as best practices for responding to a breach of PII.

P. ***Data Breaches:*** VENDOR shall notify CLIENT in writing as soon as commercially practicable, however no later than forty-eight (48) hours, after VENDOR has either actual or constructive knowledge of a breach which affects CLIENT's Data (an "Incident") unless it is determined by law enforcement that such notification would impede or delay their investigation. VENDOR shall have actual or constructive knowledge of an Incident if VENDOR actually knows there has been an Incident or if VENDOR has reasonable basis in facts or circumstances, whether acts or omissions, for its belief that an Incident has occurred. The notification required by this section shall be made as soon as commercially practicable after the law enforcement agency determines that notification will not impede or compromise the investigation. VENDOR shall cooperate with law enforcement in accordance with applicable law provided however, that such cooperation shall not result in or cause an undue delay to remediation of the Incident. VENDOR shall promptly take appropriate action to mitigate such risk or potential problem at VENDOR's expense. In the event of an Incident, VENDOR shall, at its sole cost and expense, restore the Confidential Information, to as close its original state as practical, including, without limitation any and all Data, and institute appropriate measures to prevent any recurrence of the problem as soon as is commercially practicable.

Q. ***Employee and Subcontractor Qualifications:*** VENDOR shall ensure that its employees and all subcontractors who have potential access to CLIENT Data have undergone appropriate background screening and possess all needed qualifications to comply with the terms of this Agreement. Further, all employees and subcontractors are subject to the same FERPA compliance in relation to the

'school official' designation, and should receive training that the re-disclosure of PII and/or Confidential Information will violate federal and state laws and may result in criminal and/or civil penalties.

R. *Governing Law:* This agreement shall be governed by and construed in accordance with the laws of STATE excluding its choice of law rules.

S. *Compliance:* In addition to complying with FERPA and the Maryland Education Code cited above, the VENDOR shall ensure that its products and services comply with the Federal Protection of Pupil Rights Act (34 CFR Part 98), the Federal Children's Internet Protection Act (47 CFR 54.520), and the Federal Children's Online Privacy and Protection Act (16 CFR Part 312).

T. *Limitation of Liability:* VENDOR shall be liable for any and all damages, costs and attorneys' fees which CLIENT may incur as a result of any claims, suits and judgments against CLIENT which arise out of any gross negligence or willful misconduct of the VENDOR, its employees, servants, representatives or agents during the term of this Agreement.

CLIENT: By: _____
                              Signature

                              _____
                              Printed Name   Title

                              _____
                              Date

                              _____
                              Address

VENDOR: By: _____
                              Signature

                              _____
                              Printed Name   Title

                              _____
                              Date

_____
Vendor Name

_____
Address

_____
City, State   Zip Code