STUDENT DATA PRIVACY SPECIAL TERMS AND CONDITIONS ADDENDUM

This Student Data Privacy Special Terms and Conditions Addendum (“Addendum”) is between the District and Contractor, as previously identified in the attached Agreement. It is understood and agreed that the Contractor is performing institutional services and functions that will require student data to perform those services and functions (“Services”). It is further understood that the District controls the notification to parents and guardians regarding the release of student information to providers. This Addendum is issued to expand the definitions within and provide supplemental terms and conditions to the Agreement.

1. Definition, Use and Treatment of "Data"

In the course of performing Services, Contractor will obtain confidential student data. Student data includes all Personally Identifiable Information ("PII"), directory data, confidential student record information, and other non-public information. This data includes, but is not limited to student data, meta data (e.g. logs, cookies, web beacons, etc.), and user content ("Data Files"). Any data or metadata a 3rd party will collect (e.g. analytics, etc.) is a function of the use of the provider's service.

2. Data De-Identification

De-identified Confidential Data will have all direct and indirect personal identifiers removed, including any data that could be analyzed and linked to other data to identify the student or family member / guardian. This includes, at a minimum the following: student name, address, telephone numbers, email addresses, photograph, place and date of birth, attendance record, grade level, course enrollment information, physical descriptors and user ID number (or other unique personal identifier as necessary to participate in the services provided under this Agreement).

Furthermore, Contractor agrees not to attempt to re-identify de-identified Confidential Data and not to transfer de-identified Confidential Data to any party unless:

(a) That party agrees in writing not to attempt re-identification, and

(b) Contractor gives prior written notice to District and District provides prior written consent.

Contractor may use de-identified Confidential Data for internal product development and improvement, research, and with a written commitment of Contractor to compliance with current and future applicable laws. The following information may be retained and utilized by the Contractor in a de-identified format for Contractor internal purposes: attendance record, course enrollment information, and grade level.

3. No Marketing or Advertising

Contractor is prohibited from using Confidential Data to:

(a) Market or advertise to students or families / guardians;

(b) Inform, influence or enable marketing, advertising or other commercial efforts by a third party; or

(c) Develop a profile of a student, family member / guardian or group, for any commercial purpose other than providing the Service to District.

4. Notification of Amendments to Policies

4.1. Contractor shall not change how Confidential Data is collected, used or shared under the terms of the Agreement, without advance written notice to the stated Agreement point(s) of contact for Notice and prior written consent from District.

4.2. Contractor shall provide prior written notice to District of any material changes to its terms of service, terms and conditions of use, license agreement and/or privacy policies that would alter the way student data, designated as confidential or not, is collected, stored, handled, disseminated or distributed, at least thirty (30) days prior to the implementation of any such change. District must approve changes in writing, which will not be unreasonably withheld.

4.3. It is understood and agreed that only the terms and conditions set forth in the Agreement, inclusive of this Addendum, as duly executed between the District and Contractor, will be binding, regardless of whether a student or other user “accepts” the terms and conditions presented upon logging in, an email notification is generated or a revision is posted to the Contractor’s website.

5. Data Collection

Contractor will only collect, process and store the Confidential Data that is necessary and provided by the District in order to provide Service(s) to the District under this Agreement. Contractor will not attempt to or collect, process or store Confidential Data or other data related to students, families or guardians, which is or may be available from third parties. To do so will be viewed as a material breach of the Addendum and will be handled in accordance with the Agreement.

6. Data Analysis and Mining

Contractor is prohibited from analyzing or mining Confidential Data for any purpose other than delivering the Service to District under this Agreement, or improving the Service for District. Analysis and mining of Confidential Data to support marketing, advertising or other commercial ventures, whether by Contractor or a third party, are prohibited.

7. Data Sharing and Re-Disclosure

7.1 District understands that Contractor may rely on one (1) or more sub-contractors to provide the Service under this Agreement, which may have access to Confidential Data.
At all times, the Contractor warrants and agrees to be held liable and fiscally responsible for the deliberate and/or unintentional acts and/or omissions of sub-contractors utilized in the performance of these Services who fail to adhere to the requirements for data confidentiality and security contained in the executed Agreement between the District and Contractor.

7.2 Contractor is also prohibited from further disclosing any Confidential Data unless re-disclosure is:
(a) Only in furtherance of providing the Service to District, and recipients of re-disclosed Confidential Data agree in writing to comply with the terms of this Student Data Privacy Special Terms and Conditions and related federal and state laws / regulations that protect Confidential Data, or;
(b) Required to ensure legal and regulatory compliance, or;
(c) In response to a judicial process in a court in the state of Florida, or;
(d) To protect the privacy of Confidential Data, the safety of users or others, or the security of the Service.

If any of the four (4) permitted re-disclosure events noted above occurs, Contractor will immediately notify District in writing to the person(s) listed in the "Notices" section of the Agreement. Such notification, notwithstanding unforeseen events, will occur no later than three (3) business days from notice of request to Contractor.

8. Data Transfer and Destruction

Upon notice from District, Contractor will ensure that:
(a) A complete, readable and usable copy of all Confidential Data in Contractor's possession will be delivered to District within sixty (60) days or as otherwise noted in a mutually executed migration plan, following notice from District, and;
(b) This copy of all Confidential Data will be provided in a standard format with standard delimiters and a matching data dictionary, mutually agreeable and sufficient to enable efficient transfer of the Confidential Data to a new system, and;
(c) This copy must include all Confidential Data which may have been re-disclosed to or held by sub-contractors or agents of Contractor, and;
(d) Following notice of acceptance of this copy of all Confidential Data by District, Contractor will permanently destroy all copies of Confidential Data held by Contractor or re-disclosed by Contractor, e.g. to Contractor's agents, sub-contractors or business partners. Permanent destruction of this Confidential Data must be non-recoverable. It is

recommended that the Contractor meet either the Department of Defense ("DoD") standard 5220.22-M or the processes recommended by National Institute of Standards and Technology ("NIST") Special Publication 800-88, and;

(e) Within ninety (90) days of notice, Contractor will deliver a written confirmation to District certifying that the permanent destruction of all Confidential Data held by Contractor and Contractor's sub-contractors, agents and business partners has been completed.

9. Rights and License to Confidential Data and Intellectual Property

The parties agree that:

(a) All rights to Confidential Data and derivative works created from Confidential Data shall remain the exclusive property of District, and;

(b) All rights to District intellectual property shall remain the exclusive property of District and District students and staff, and;

(c) Contractor may not transfer Confidential Data or District intellectual property to any third party without prior written authorization from the District, and;

(d) District grants to Contractor a limited, nonexclusive license to use, process and store the Confidential Data and District intellectual property solely for the purpose of delivering the Service to District under the terms of the Agreement, and;

(e) This limited, nonexclusive license granted to Contractor by District expires when the Agreement is terminated unless otherwise agreed to in writing between Contractor and District resulting from a mutually executed migration document.

10. Confidential Data: Access, Changes, Copies and Removal

At any time and upon District's request, any Confidential Data held by Contractor will be made available to District, may be changed by District, may be deleted in whole or in part by District, and may be copied by District.

11. Security Framework and Standards

Contractor will operate the Service and collect, process and store Confidential Data in accordance with NIST data security standards and current industry best practices, and maintain all technologies, policies, procedures and practices necessary to secure and protect the confidentiality and integrity of Confidential Data, and prevent unauthorized access, disclosure and use. Contractor will, at a minimum:

(a) Restrict access to the Service and Confidential Data to only those individuals that require access in order for Contractor to provide the Service to District, and;

(b) Establish user IDs and authentication as necessary to protect access to Confidential Data, and protect all such user credentials from unauthorized access or use, and;

(c) Always protect all Confidential Data with strong encryption, at rest and in transit, and;

(d) Prevent hostile or unauthorized intrusion that could compromise confidentiality, result in data corruption, or deny access to or the proper operation of the Service, and;
(e) Prevent and detect computer viruses and malware from spreading through the use of the Service, e.g. via e-mail, files, documents, messages, other data or the required use of insecure client-side applications, and;
(f) Detect and prevent the unauthorized re-disclosure of Confidential Data by Contractor employees or agents, and;
(g) Provide prior notice to District of any planned system change that may impact the security of Confidential Data.

Contractor acknowledges and agrees that this Agreement is for the purpose of sharing Data Files between the parties in a manner consistent with the Family Educational Rights and Privacy Act ("FERPA"). The Data Files will be used by the Contractor and its employees to populate student data only for the purpose of delivering these Services. Contractor further acknowledges and agrees that all copies of such Data Files, including any modifications or additions to Data Files or any portion thereof from any source, are subject to the provisions of this Agreement in the same manner as the original Data Files.

12. Data Breach

In the event of an unauthorized disclosure of Confidential data, Contractor shall, pursuant to the following procedure: notify District in writing to: ECSDdatabreach@escambia.k12.fl.us within three (3) days of its determination that it has experienced a data breach, breach of security, privacy incident or unauthorized acquisition or use of any Data Files and/or any portion thereof contained therein. Contractor is aware and agrees that this is the only instance in which email notification is accepted and only in relation to actual, suspected, or potential data breaches. Any other use of this email for notification, including changes to Terms and Conditions, Privacy, etc. are hereby dismissed and will not constitute an approved change to the Agreement. Contractor agrees that said notification shall include, to the extent feasible, the date or approximate dates of such incident and the nature thereof, the specific scope of said breach (i.e., what data was accessed, used, released or otherwise breached, including the names of individual students that were affected by said breach) and what actions or steps with respect to the incident that Contractor plans to take or has taken in response to said breach. Additionally, Contractor agrees to adhere to all requirements in federal law with respect to a data breach related to the Data Files, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach. Contractor 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 data breach, breach of security, privacy incident or unauthorized acquisition or use of Data Files or any portion thereof, including personally identifiable information and agrees to provide District, upon request, with a copy of said written incident response plan.