

## **ADDENDUM**

This Addendum is agreed and entered into by and between the **Boone County School District** (“District”) and \_\_\_\_\_ (“Vendor”), and is intended to amend, modify, and supplement the \_\_\_\_\_ (hereinafter, the “Agreement”).

**WHEREAS**, the Vendor is providing educational or digital services to the Boone County Board of Education and, by extension, the District; and

**WHEREAS**, the Vendor and the District recognize the need to protect personally identifiable student information, and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act (“FERPA”), 20 U.S.C. § 1232(g), 34 C.F.R. Part 99; the Children’s Online Privacy Protection Act (“COPPA”), 15 U.S.C. § 6501-6506, 16 C.F.R. Part 312; the Protection of Pupil Rights Amendment (“PPRA”), 20 U.S.C. § 1232h; 34 C.F.R. Part 98; and applicable state privacy laws and regulations; and

**WHEREAS**, the Vendor and District desire to enter into this Addendum for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations, and to amend, modify, and supplement the Agreement previously entered into; and

**NOW THEREFORE**, in consideration of the of the terms, covenants, conditions and promises set forth herein, as well as those set forth in the Parties’ Agreement, and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties agree to amend, modify, and supplement the Agreement as follows:

**Section 1. Definitions for Addendum.** For the purpose of this Addendum, the following definitions shall apply:

- 1.1 “Confidential Student Information” shall mean all information, whether PII or directory information, included in the Education Records provided to or accessed by Vendor pursuant to the terms of the Parties’ Agreement.
- 1.2 “District Data” shall mean any information or data owned by the District and provided to Vendor pursuant to the Parties’ Agreement.
- 1.3 “Education Records” shall be defined consistent with the definition set forth in 20 U.S.C. § 1232g(a)(4)(A); 34 C.F.R. § 99.3, and shall mean records that are: (1) directly related to a student; and (2) maintained by an educational agency or institution or by a party acting for the agency or institution.

1.4 “Personally Identifiable Information” (“PII”) shall be defined consistent with the definition set forth in 20 U.S.C. § 1232g(a); 34 C.F.R. § 99.3, and shall mean identifiable information that is maintained in education records and includes direct identifiers, such as a student’s name or identification number, indirect identifiers, such as a student’s date of birth, or other information which can be used to distinguish or trace an individual’s identity either directly or indirectly through linkages with other information.

**Section 2. Student Privacy Acknowledgements.** The Parties acknowledge the following: (a) the District is a public school district and is subject to the Family Educational Rights and Privacy Act (“FERPA”), 20 U.S.C. § 1232g; 34 CFR Part 99, which protects the privacy of student education records; (b) the District has outsourced certain services to Vendor, as defined in the Agreement, in furtherance of a legitimate educational interest that would otherwise be performed by the school district; (c) these services include the collection and storage of certain District Data and Confidential Student Information, as set forth in Section 1 of this Addendum; (d) the Vendor is under the direct control of the District with respect to the use and maintenance of District Data and Confidential Student Information provided to it pursuant to the Parties’ Agreement; and (e) Vendor is subject to the requirements in FERPA that any PII obtained from Education Records may be used only for the purposes for which the disclosure was made and consistent with the terms of the Parties’ Agreement.

**Section 3. Vendor’s Obligations.** Vendor acknowledges and agrees to the following: (a) Vendor is acting as a contractor to the District in performing the function, either directly under the terms of the Agreement and this Addendum, or indirectly through Vendor’s interfaces with another District contractor; (b) Vendor uses reasonable methods to ensure that only individuals with a legitimate educational interest (as to a particular student, such as the student, his or herself, the student’s guardian, and the District) shall have access to the District Data in Vendor’s possession or control; and (c) Vendor uses reasonable methods to ensure that no third parties shall have access to Confidential Student Information or Education Records in its control unless written authorization to distribute such information is provided by the student’s parent/guardian.

**Section 4. Ownership of Data.** As between District and Vendor, the District retains ownership of all data provided to Vendor pursuant to the Parties’ Agreement, regardless of whether such data is provided to Vendor by the District, its students, parents, guardians, or any other authorized user.

**Section 5. Data Transmission.** The Vendor shall ensure the secure transmission of any data exchanged during the course of this agreement. All data transmissions, whether internal or external, shall be encrypted using encryption processes for data in motion

which comply, as appropriate, with National Institute of Standards and Technology (“NIST”) Special Publications 800-52; NIST Special Publications 800-77; NIST Special Publications 800-113, or others which are Federal Information Processing Standards (“FIPS”) 140-2 validated, to protect the confidentiality and integrity of the transmitted data. In the event of any security incidents or breaches affecting data while in transit, the Vendor agrees to promptly notify BCS and take necessary remedial actions to mitigate the impact as set forth in Section 8 of this Addendum.

**Section 6. Security of Data at Rest.** Vendor acknowledges that it is responsible for implementing robust measures to safeguard data at rest. This includes, but is not limited to, encryption of stored data, physical/logical access controls, regular security audits, and the prohibition of storing any data onto a personally owned device. All District Data must be stored in a secure environment, with access limited to authorized personnel only. Vendor shall adhere to valid encryption processes for data at rest that are consistent with NIST Special Publication 800-111 and comply with relevant data protection regulations to ensure the confidentiality and integrity of data at rest. If requested by the District, Vendor shall provide a list of locations where student data is/may be stored, and whenever possible, including where required by applicable law, data shall be stored within the United States. In the event of any security incidents or breaches affecting data at rest, the Vendor agrees to promptly notify the Client and take necessary remedial actions to mitigate the impact.

**Section 7. Prohibition Against Use of Student or District Likeness.** Vendor acknowledges and agrees that it may not disseminate the District’s name, logo, or likeness for any reason, including marketing, internal training, or similar purposes, to any third party without written authorization from the District. Vendor further acknowledges and agrees that it may not disseminate any Confidential Student Information or District Data – whether explicitly protected under FERPA, directory information (i.e., name, grade, etc.), or student likeness – without written authorization from the student or, if the student is a minor, the student’s parent/guardian. Vendor shall not in any case process student data to advertise or facilitate advertising or to create or correct an individual or household profile for any advertisement purpose, and shall not sell, disclose, or otherwise process student data for any commercial purpose as defined by KRS 365.734.

**Section 8. Security Breach Remediation and Notice.** Vendor agrees to maintain procedures and practices to preemptively safeguard against security breaches as described in KRS 61.932. However, in the event of a security breach as defined by KRS 61.931, Vendor shall notify the District in the most expedient time possible and without unreasonable delay, but within seventy-two (72) hours of determination of a security breach relating to the personal information in the possession of Vendor. The notice to the District shall

include all information the nonaffiliated third party has with regard to the security breach at the time of notification. In the event of a security breach relating to the personal information in the possession of Vendor, Vendor shall bear the full cost of the notification and investigation requirements set forth in KRS 61.933. In the event of a suspected or confirmed breach, Vendor agrees to retain an independent IT consulting firm, which is mutually agreed-upon by the Parties, to provide requisite forensic/recovery/notification services as provided for by the Commonwealth Office of Technology's recommended data breach response plan. Vendor agrees to comply with all provisions of KRS 61.931-.934 pertaining to the prevention of, investigation of, response to, and remediation of any and all such security breaches.

**Section 9. Cloud Computing Service Providers.** If Vendor is a cloud computing service provider (as defined in KRS 365.734(1)(b) as "any person other than an educational institution that operates a cloud computing service"), Vendor agrees that: (a) Vendor shall not process Confidential Student Information or student data as defined by KRS 365.734 for any purpose other than providing, improving, developing, or maintaining the integrity of its cloud computing services, unless Vendor receives express permission from the student's parent. Vendor shall work with the student's school and the District to determine the best method of collecting parental permission; (b) Vendor shall not in any case process student data to advertise or facilitate advertising or to create or correct an individual or household profile for any advertising purposes; (c) Vendor shall not sell, disclose, or otherwise process Confidential Student Information for any commercial purpose; and (d) Vendor shall certify in writing to the District that it will comply with KRS 365.734(2).

**Section 10. Advertising Limitations.** Vendor is prohibited from using, disclosing, or selling Confidential Student Information or District Data to (a) inform, influence, or enable targeted advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the services as set forth in the Parties' Agreement. This section does not prohibit Vendor from using Confidential Student Information or District Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or District employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Confidential Student Information or District Data for any purpose explicitly permitted by the Parties' Agreement.

**Section 11. Open Records.** Vendor acknowledges that the District is subject to the Kentucky Open Records Act, KRS 61.870 to KRS 61.884, and may be required to disclose certain information obtained pursuant to the Parties' relationship as set forth therein.

Vendor agrees that it will not pursue any legal action against the District for any disclosure of Vendor's information or data made in response to an Open Records Request.

**Section 12. Law Enforcement or Court-Mandated Disclosures.** Should law enforcement or other government entities ("Requesting Part(ies)") contact Vendor with a request for Confidential Student Information or Education Records held by the Vendor pursuant to the Parties' Agreement, the Vendor shall notify the District in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the Board of the request. Similarly, if Vendor becomes legally compelled to disclose any District Data, Confidential Student Information, or Education Records (whether by judicial or administrative order, applicable law, rule, regulation, or otherwise), Vendor shall use all reasonable efforts to provide the District with advance notice before disclosure so that the District may seek a protective order or other appropriate remedy to prevent the disclosure or to ensure the Board's compliance with the confidentiality requirement of federal or state law.

**Section 13. Data Protection Upon Conclusion of Contract.** Upon termination, cancellation, expiration, or other conclusion of the Parties' Agreement, Vendor shall return all District Data in the possession of Vendor, its subcontractors, or agents to the District, unless otherwise directed by the District in writing that such Client Data alternatively be destroyed. Vendor shall complete such return or destruction within thirty (30) calendar days of the termination of this Agreement and shall certify compliance with this Section, in writing, to the District within ten (10) calendar days of such return or destruction.

**Section 14. Insurance.** Vendor shall maintain, during the term of the Agreement, a cyber-insurance liability policy, in the amount of \$3 million. Upon request, Vendor shall furnish the certificate of insurance evidencing this coverage. The certificate of insurance shall name the Boone County Board of Education as additional insured in the Description of Operations section of the Certificate of Insurance.

**Section 15. Equitable Relief.** In any action or proceeding to enforce rights under the Agreement, the prevailing party will be entitled to recover costs and attorneys' fees. Vendor acknowledges that the District may seek and obtain injunctive relief for the unauthorized use or dissemination of District Data or Confidential Information, or other violations of the Parties' Agreement, in addition to, and not in limitation of, other legal remedies provided under state and federal law.

**Section 16. Governance.** The laws of the Commonwealth of Kentucky shall govern all questions as to the execution, validity, interpretation, construction and performance of this Agreement and Addendum, or any of their terms. Any suit, action or other proceeding regarding the execution, validity, interpretation, construction or performance of this agreement shall be filed in the Boone Circuit Court of the Commonwealth of Kentucky. In

the event of litigation in a U.S. District Court, venue shall lie exclusively in the Eastern District of Kentucky.

**Section 17. Effect of Addendum.** The Parties agree that the terms and conditions set forth in this Addendum modify, amend, and supplement the Agreement as set forth above, and agree to be bound to the terms herein. To the extent that the Addendum expressly conflicts with the terms and conditions of the Agreement, the Addendum shall control.

**IN WITNESS WHEREOF,** the District and Vendor execute this Addendum to be effective consistent with the effective date of the Parties' Agreement.

**BOONE COUNTY SCHOOL DISTRICT**

By: \_\_\_\_\_

Date: \_\_\_\_\_

Printed Name: \_\_\_\_\_

Title/Position: \_\_\_\_\_

**[VENDOR NAME HERE]**

By: \_\_\_\_\_

Date: \_\_\_\_\_

Printed Name: \_\_\_\_\_

Title/Position: \_\_\_\_\_