



Services Order Form

Order #: Q-413556-2
Date: 2025-01-27
Offer Valid Through: 2025-06-29

6330 South 3000 East, Suite 700, Salt Lake City, UT 84121, United States

Order Form For Boone County School District (KY)

Address: 8330 US Highway 42
City: Florence
State/Province: Kentucky
Zip/Postal Code: 41042
Country: United States

Order Information

Billing Frequency: Annual Upfront
Payment Terms: Net 30

Billing Contact

Name: _____
Email: _____
Phone: _____

Primary Contact

Name: Stephanie Younger
Email: stephanie.younger@boone.kyschools.us
Phone: +1 859 283 1003

Billing Frequency Term:

Non-Recurring items will be invoiced upon signing. Recurring items will be invoiced 30 days prior to the annual start date.

Year 1						
Description	Start Date	End Date	Metric	Qty	Price	Amount
Canvas LMS Cloud Subscription	2025-06-30	2026-06-29	User	14,000	USD 4.62	USD 64,680.00
24x7 Support	2025-06-30	2026-06-29	20% of Subscription (Minimums Apply)	1	USD 12,936.00	USD 12,936.00
Recurring Sub-Total						USD 77,616.00
Year 1 Total						USD 77,616.00
Grand Total:						USD 77,616.00

Deliverable	Description	Expiration	Qty
Canvas LMS Cloud Subscription	Canvas LMS Cloud Subscription: Per User	N/A	14,000
24x7 Support	24x7 support per year (20% of subscription - minimums apply)	N/A	1

The items above must be completed during the time period beginning on the later of the Effective Date or the initial Start Date specified in this Order Form and ending pursuant to the time frame set forth in the Expiration column above.

Metrics and Descriptions:

User: User Metric reflects the maximum number of individuals authorized by the Customer to access and/or use the Service and Customer has paid for such access and/or use.

In the event Customer enables access to the Service to more Users over a given contract year than are allocated to such contract year as set forth above, then Instructure reserves the right, in its sole discretion, to invoice the Customer for such additional number of Users. In addition, the User fees set forth above are based on the assumption that Customer's Users will use the Service commensurate with the average usage patterns of users across Instructure's user base in the aggregate (such average usage being referred to herein as "Typical Use") and do not account for usage of the Service by Customer's Users beyond such Typical Use. To the extent the Users' usage of the Service, in the aggregate, exceeds the Typical Use at any given time, Instructure reserves the right, in its sole discretion, to increase the fees by an amount proportional to such excess usage. In the event Instructure increases the fees pursuant to this paragraph, Instructure shall send an invoice to Customer for the applicable increase along with documentation evidencing the additional usage of or additional Users who have access to the Service giving rise to such fee increase. Any invoice sent pursuant to the foregoing shall be due and payable within 30 days of receipt.

Duration: The Services provided under this Order Form shall begin on the first year Start Date set forth above and continue through the last year End Date set forth above, provided, however, that Instructure may provide certain implementation related Services prior to the first year Start Date at its sole discretion.

Miscellaneous: Instructure's support terms are available as follows:
Canvas & Catalog: <https://www.instructure.com/canvas/support-terms>

As part of our commitment to provide the most innovative and trusted products in the industry, at times we must increase our renewal rates to cover additional expenses associated with advancing our products. If you have concerns with any increases, please reach out to your account representative.

In the event that Customer fails to execute this Order Form prior to the Start Date listed above, all fees shall become due payable upon Customer's receipt of an invoice.

Terms and Conditions

This Order Form shall be governed by the Master Terms and Conditions which can be found here:
<https://www.instructure.com/policies/mastertermsconditions>.

Product Specific Supplements which can be found here: <https://www.instructure.com/policies/product-supplements>, govern the use of the applicable product and/or feature offerings listed in this Order Form and/or utilized by Customer, and are incorporated into the Master Terms and Conditions.

In the event of any conflict between this Master Terms and Conditions and any addendum thereto and this Order Form, the provisions of this Order Form shall control.

The parties agreement with regards to Instructure's processing of personal data or personally identifiable information can be found at: <https://www.instructure.com/policies/data-processing-addendum>

PURCHASE ORDER INFORMATION	TAX INFORMATION
Is a Purchase Order required for the purchase or payment of the products on this order form?	Check here if your company is exempt from US state sales tax : _____
Please Enter (Yes or No): _____	<i>Please email all US state sales tax exemption certifications to ar@instructure.com</i>
If yes, please enter PO Number: _____	

Customer purchasing documentation, such as Purchase Orders, shall only be used as proof of acceptance of the Order Form referenced therein, and the associated Master Terms and Conditions. Any terms and conditions included in any such Customer purchasing documentation are hereby expressly disclaimed by Instructure, shall be void and of no effect, and shall in all cases be superseded by the applicable Master Terms and Conditions.

By executing this Order Form, each party agrees to be legally bound by this Order Form.

Boone County School District (KY)

Signature:	
Name:	
Title:	
Date:	

Instructure, Inc.

Signature:	
Name:	
Title:	
Date:	

Data Privacy and Security Agreement

This Data Privacy and Security Agreement ("Agreement") is agreed and entered into by and between the Boone County School District ("District") and Instructure, Inc. ("Vendor") on this the 1 day of April, 2025.

WHEREAS, Boone County School District ("District") is a public school district organized and existing under and pursuant to the constitution and laws of the State of Kentucky and with a primary business address at 8330 US Highway 42, Florence, KY 41042; and

WHEREAS, Vendor has been contracted in terms of a services order form or other agreement executed between the Parties (the "Services Agreement") to perform certain educational services as described fully in Exhibit A ("Provided Services") with a primary place of business at 6330 South 3000 East, Suite 700, Salt Lake City, UT, United States, 84121; 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 Agreement for the purpose of establishing their respective obligations and duties in order to comply with applicable regulations; and

WHEREAS, the Parties acknowledge that this Agreement shall amend, modify, and supplement any agreement or terms previously entered into; and

NOW THEREFORE, in consideration of the of the terms, covenants, conditions and promises set forth herein, and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties agree as follows:

Section 1. DEFINITIONS

1.1 "Confidential Student Information" shall mean any information or material, in any medium or format, included in the Education Records provided to or accessed by the Vendor pursuant to the terms of the Services Agreement. Confidential Student Information includes both PII and directory information.

1.2 "De-identified Data" shall mean data that has a re-identification code and has enough personally identifiable information removed or obscured so that the remaining

information does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual. The re-identification code may allow the recipient to match information received from the same source.

1.3 “District Data” shall mean any information or data owned by the District and provided to Vendor pursuant to the Services Agreement, including but not limited to Confidential Student Data and PII. District Data shall not include De-Identified Data.

1.4 “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.

1.5 “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.

1.6 “Personal Information” shall be defined in accordance with KRS 61.931(6) as an individual’s first name or first initial and last name; personal mark, or unique biometric or genetic print or image in combination with one (1) or more of the following data elements: (1) an account, credit card number, or debit card number that in combination with any required security code, access code or password, would permit access to an account; (2) a Social Security number; (3) a taxpayer identification number that incorporates a Social Security number; (4) a driver’s license number, state identification card number, or individual identification number issued by an agency; (5) A passport number or other identification number issued by the United States Government; or (6) Individually Identifiable Information as defined in 45 C.F.R. 160.013 (of the Health Insurance Portability and Accountability Act), except for education records covered by FERPA.

1.7 “security breach” shall have the same definition as under KRS 61.931(9).

Section 2. PURPOSE AND SCOPE

2.1 The purpose of this Agreement is to allow the District to provide the Vendor with student and teacher PII data and the subsequent processing of the data.

2.2 This Agreement is meant to ensure the Vendor and the District recognize the need to protect PII, 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

2.3 This Agreement shall be effective as of the date upon which it is signed by both parties (“Effective Date”), and shall automatically renew from year to year until such time that Vendor’s provision of the Provided Services to the District are not renewed or expire or are terminated pursuant to the Parties’ Services Agreement.

2.4 The laws of the Commonwealth of Kentucky and shall govern all questions as to the execution, validity, interpretation, construction, and performance of this Agreement and any of its 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, the venue shall lie exclusively in the Eastern District of Kentucky.

Section 3. DISTRICT DUTIES

The District shall provide data as required for Vendor to conduct its Provided Services and shall be in compliance with all applicable federal, state, and local privacy laws, rules, and regulations. District shall be responsible for providing all notices and obtaining all consents and rights necessary under applicable laws for the Vendor to process data in relation to the Provided Services, including securing any parent permissions regarding the use of Confidential Student Information or PII.

Section 4. VENDOR DUTIES

4.1 Vendor acknowledges that the District has outsourced certain services to Vendor, as defined above as Provided Services, in furtherance of a legitimate educational interest that would otherwise be performed by the school district. These Provided Services necessitate the collection and storage of certain District Data and Confidential Student Information. Vendor shall act as a contractor to the District in performing the Provided Services, either directly under the terms of any service or licensing agreement related to the Provided Services, or indirectly through the Vendor’s interfaces with another District contractor, and Vendor therefore acknowledges that it 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 solely for the purpose of performing the Provided Services.

4.2 Vendor shall implement commercially reasonable methods to ensure that District Data is accessed, used, and manipulated exclusively by authorized individuals with a legitimate educational interest—such as the student, the student’s guardian, and the

District—or by personnel essential for the successful performance and execution of the Provided Services. No unauthorized third parties shall have access to Confidential Student Information or Education Records in Vendor’s control unless written authorization to distribute such information is provided by the student’s parent/guardian. Notwithstanding anything to the contrary in this Agreement, Vendor is permitted to engage third parties to provide elements of the Provided Service to enable Vendor to fulfill its obligations under the Services Agreement, and the District acknowledges and agrees that District Data will be shared with such third parties for this purpose. The Vendor agrees that it shall require each of such third parties to enter into written agreements containing obligations of confidentiality that are no less stringent than those set forth in this Agreement. Vendor further agrees that, within ten (10) business days of receiving a written request from the District, it shall furnish to District a list of all third parties who have access to District Data pursuant to this Section. In the event that Vendor engages a third party to provide elements of the Provided Service and shares District Data with said third party, Vendor shall indemnify the District, its officers, directors, employees, and agents for Reasonable Out of Pocket Remediation Costs arising from the third party’s negligence or intentional misconduct resulting in an actual or reasonably suspected security breach of District Data. “Reasonable Out of Pocket Remediation Costs” consist of: (a) reasonable out-of-pocket expenses for legally-required notifications of District’s end-users (but not the costs of any other professional third-party services, including those relating to crisis management, public relations or media relations services, which are considered as consequential loss); and (b) actual costs of payments, fines, penalties, or sanctions imposed on the District by a court, tribunal, arbitration panel, government body or regulatory agency for such security breach.

4.3 Vendor shall likewise implement commercially reasonable measures to safeguard District Data at rest, and advise all individuals accessing such data on proper procedures for securely maintaining data. Vendor shall adhere to valid encryption processes for data at rest that are consistent with industry standards and comply with relevant data protection regulations to ensure the confidentiality and integrity of data at rest. If requested by the District, the Vendor shall provide a list of locations where District Data is/may be stored, and whenever possible, including where required by applicable law, District Data shall be stored within the United States.

4.4 The Vendor shall ensure the secure transmission of any District Data exchanged pursuant to the Provided Services. All District Data transmissions in and out of the Provided Services are encrypted using TLS (v1.2 or later) forward-secrecy-compliant ciphers (e.g. ECDHE-ECDSA-AES128-GCM-SHA256), , to protect the confidentiality and integrity of the transmitted data. In the event of any security incidents affecting District Data while in transit when being routed by Vendor or Vendor's content delivery network, the Vendor agrees to promptly notify the District and take necessary remediation actions to mitigate the impact.

4.5 In the event of any security incidents or reasonably suspected or actual breaches affecting the security of District Data, the Vendor agrees to promptly notify the District and take necessary remedial actions to mitigate the impact as set forth in Section 6 of this Agreement.

4.6 Following 90 days after the termination, cancellation, expiration, or other conclusion of the Services Agreement, or upon receipt of written request from District, Vendor shall delete all Confidential Student Data in its possession. Vendor shall complete such destruction within a reasonable period of the receipt of the written request and shall, upon request, certify compliance with this Section, in writing, to the District within ten (10) calendar days of such destruction.

4.7 Vendor is prohibited from using, disclosing, or selling Confidential Student Information or District Data to any unauthorized individual or entity, or for any purpose which is not required in the performance of Vendor's Provided Services. This does not prohibit Vendor from using Confidential Student Information or District Data: (a) for adaptive learning or customized student learning (including generating personalized learning recommendations); (b) to make product recommendations to teachers or District employees who have voluntarily subscribed to Vendor's Provided Services; (c) to notify account holders about new education product updates, features, or services; or (d) from otherwise using Confidential Student Information or District Data for any purpose explicitly permitted by the Parties' Agreement. However, 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.

4.8 Other than as set out in the Agreement, Vendor 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 likewise 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. Notwithstanding the foregoing, (i) Vendor shall be allowed to use District's name as part of customer lists, so long as it does not state expressly or implies that the District endorses Vendor; and (ii) in the event the Vendor is a publicly traded company, Vendor may disclose the relationship with the District in its public filings and disclosures.

4.9 Vendor shall maintain, during the term of the Agreement, a Technology Errors and Omission (cyber-insurance) liability policy, in the amount of \$3 million. Upon request, the Vendor shall furnish the certificate of insurance evidencing this coverage.

4.10 To the extent permitted by law, Vendor assumes all liability for damages which may arise from its use, storage, or disposal of the District Data in a manner that breaches the provisions of this Agreement. The District shall not be liable to the Vendor for any loss, claim or demand made by the Vendor, or made against the Vendor by any other party, due to or arising from the use of data by the Vendor, except to the extent permitted by law when caused by a breach of this Agreement or the Services Agreement, gross negligence or willful misconduct of the District.

Section 5. OWNERSHIP OF DATA

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

Section 6. SECURITY BREACH REMEDIATION AND NOTICE

6.1 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 confirmed or suspected security breach as defined by KRS 61.931, Vendor shall notify the District of within seventy-two (72) hours of determination of a security breach or suspected breach relating to the Personal Information or Confidential Student Information in the possession of Vendor. The notification shall include, at a minimum (to the extent available), the following information to the extent known by the Vendor and as it becomes available: (a) the name and contact information of the individual reporting a breach to this section; (b) the date of the breach, or estimated date if not yet confirmed; (c) a list of the information and data reasonably believed or confirmed to have been subject of the breach; (d) a list of the students whose information is believed to have been affected; and (e) a general description of the breach incident.

6.2 The Vendor further acknowledges and agrees to maintain a written incident response plan that reflects standard practice and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incidents or unauthorized acquisition or use of confidential information and agrees to provide the District, upon request, with a summary of said written response plan.

6.3 In the event of a security breach relating to Personal Information or Confidential Student Information in the possession of Vendor that has resulted from a breach of the obligations of the Vendor, under this Agreement, Vendor shall bear the full cost of the notification to impacted individuals and investigation requirements set forth in KRS 61.933 in relation to Vendor's systems.

6.4 In the event of a suspected or confirmed breach of Personal Information or Confidential Student Data in the possession of Vendor, Vendor agrees to retain an independent IT consulting firm to provide requisite forensic/recovery/notification services as provided for by the Commonwealth Office of Technology's recommended data breach response plan. Within 48 hours of completion of the investigation, Vendor shall notify the District if the investigation finds that the misuse of Personal Information or Confidential Student Data occurred or is likely to occur. Upon request, Vendor shall additionally provide an executive summary of any final investigation report rendered by the independent IT consulting firm insofar as the report relates to District Data, subject to the execution of a confidentiality agreement between the parties.

6.5 Vendor agrees to adhere to applicable provisions of Kentucky Personal Information Security and Breach Investigation Procedure and Practices Act, KRS 61.932, *et seq.*, pertaining to the prevention of, investigation of, response to, and remediation of any and all security breaches related to or unauthorized disclosures of Personal Information in the possession of Vendor.

6.6 Vendor further agrees to adhere to all applicable federal and state requirements pertaining to the prevention of, investigation of, response to, and remediation of any and all security breaches related to or unauthorized disclosures of District Data and PII.

6.7 In the event of a breach originating from the District's use of Vendor's Provided Services, Vendor shall cooperate with the District to the extent necessary to expeditiously secure any data subject to an unauthorized disclosure.

Section 7. CLOUD COMPUTING SERVICE PROVIDERS

If the Vendor is a cloud computing service provider as defined in KRS 365.734(1)(b), Vendor agrees that:

- a. Vendor shall not process Confidential Student Information or any 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. Pursuant to KRS 365.734 (2), the Vendor shall not in any case process Confidential Student Information to advertise or facilitate advertising or to create or correct an individual or household profile for any advertising purpose and shall

not sell, disclose, or otherwise process confidential student data for any commercial purpose;

- c. Pursuant to KRS 365.734 (3), upon request, the Vendor shall certify in writing to the District that it will comply with KRS 365.734(2).

Section 8. NOTICES

All notices or other communication required or permitted to be given pursuant to this agreement may be given via e-mail transmission or certified mail sent to the designated representatives below.

The designated representative for the District for this Agreement is:

Name: _____ Title: _____
Address: 8330 US 42 Florence Ky 41042
Phone: 859-283-1003 Email: _____

The designated representative for the Vendor for this Agreement is:

Name: _____ General Counsel Title: _____ c/o Legal Team
Address: 6330 South 3000 East, Suite 700, Salt Lake City, Ut, United States, 84121
Phone: 1.800.203.6755 Email: privacy@instructure.com

Section 9. ASSISTANCE IN DATA DELETION

Vendor shall provide District with commercially reasonable assistance in handling a request from a student and/or their parent/guardian to delete Personal Information pertaining to such individual, to the extent (a) legally permitted, and (b) District does not have access to such Personal Information through its use or receipt of the Provided Services, taking into account the nature of the processing of Personal Information and the information available to the Vendor.

Section 10. MISCELLANEOUS PROVISIONS

10.1 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. Should the District receive a records request pertaining to the Vendor and/or the Provided Services, District shall make reasonable efforts to notify Vendor to enable Vendor to specify which information, if any, that it deems exempt from disclosure. 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 in accordance with applicable laws.

10.2 Law enforcement or court-mandated disclosures. Should law enforcement or other government entities ("Requesting Part(ies)") contact Vendor with a request for Confidential Student Data or District Data held by the Vendor pursuant any agreement of the Parties, 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 District 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 District's compliance with the confidentiality requirement of federal or state law.

10.3 Equitable Relief. 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 applicable state and federal law.

10.4 Cooperation with District Auditor. District will first use all reasonable efforts to satisfy District audit needs through (a) copies of Vendor's most recently completed SOC-2 Type II audit report and/or its public ISO 27001 certificate; (b) a summary of Vendor's operational practices related to data protection and security; (c) summary of the most recent

annual penetration test; and (d) making Vendor personnel reasonably available for security-related discussions. If the aforesaid is not sufficient, the District has the right to no more than once annually audit (either internally or via a mutually agreed third party) records of the Vendor relating to the performance of Provided Services or to data privacy processes and procedures for the purposes of meeting the District's obligations under applicable laws, provided that, District or its third-party representatives are contractually bound by obligations of confidentiality for such audit information. District must promptly provide Vendor with information regarding any non-compliance discovered during the Audit. To request an Audit, District must submit a detailed plan at least 3 weeks in advance of the proposed Audit date describing the proposed scope, duration, and start date of the Audit. Audit requests must be sent to security@Instructure.com with a copy to privacy@instructure.com. The Audit must be conducted during regular business hours, subject to Vendor's policies, and may not unreasonably interfere with Vendor's business activities. District is responsible for its own expenses in conducting an Audit.. In the event of an annual audit, Vendor agrees to reasonably cooperate with District requests.

10.5 Severability. If any provision of this Agreement is held to be invalid, illegal, or unenforceable by a court of competent jurisdiction, such invalidity, illegality, or unenforceability shall not affect the validity or enforceability of the remaining provisions of this Agreement. The parties agree that such invalid or unenforceable provision shall be modified to the extent necessary to make it valid, legal, and enforceable, and, to the greatest extent possible, that provision will be construed in a manner that reflects the original intent of the parties.

10.6 Successors Bound. This Agreement is and shall be binding upon the respective successors in interest to the Vendor in the event of a merger, acquisition, consolidation, or other business reorganization or sale of all or substantially all of the assets of such business. In the event the vendor sells, merges, or otherwise disposes of its business to a successor during the term of this Agreement, the Vendor shall provide written notice to the District no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the Agreement and any obligations with respect to confidential data within the service agreement. The District has the authority to review and address the Agreement if it disapproves of the successor to whom the Vendor is selling, merging, or otherwise disposing of its business.

10.7 Effect of Agreement. The Parties agree that the terms and conditions set forth in this Agreement modify, amend, or supplement the Services Agreement between the Parties and further agree to be bound to the terms herein. To the extent that the Agreement expressly conflicts with the terms and conditions of the Services Agreement between the Parties, this

Agreement shall control. Provided that, to the extent permitted by applicable laws, Vendor's liability arising out of or in relation to this Agreement will be subject to any aggregate limitation of liability that applies under the Services Agreement.

[Remainder of this page intentionally left blank]

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

BOONE COUNTY SCHOOL DISTRICT


By: _____

Date: 6/12/2025

Printed Name: Jesse Parks

Title/Position: Board of Ed, Chair

INSTRUCTURE, INC.

By:  _____

Date: 04/01/2025

Printed Name: Austin Holden

Title/Position: Sr Manager, Deal Desk

Exhibit A: Products and Service

This AGREEMENT covers access to and use of Instructure Inc.'s existing Provided Services that collect, process or transmit Student Data, as identified below:

Canvas LMS subscription services