Exhibit C

DATA CONFIDENTIALITY AND SECURITY AGREEMENT

INSERT FULL LEGAL NAME OF CONTRACTING PARTY ("Provider") hereby agrees to the terms of this Data Confidentiality and Security Agreement ("Security Agreement") for the purpose of sharing confidential or sensitive information between employees or agents of the Orange County Board of Education ("OCS"), and Provider (collectively, the "Parties").

1. **Definitions.**

   a. **"Services"** shall mean the services provided by Provider to OCS pursuant to attached contract.

   b. **"OCS Data."** "OCS Data" includes any data, information, records, or other content that OCS or OCS end users upload, create, modify, or share with Provider, including but not limited to any personally identifiable information ("PII") about students, employees, or other users. "OCS Data" also includes user identification information and metadata which may contain OCS Data or from which OCS Data may be ascertainable, and any de-identified data or aggregated data sets that may be generated from the underlying data provided. "OCS Data" also includes any "Student Data" as defined below.

   c. **"Student Data."** "Student Data" is a subset of "OCS Data." "Student Data" includes any data that directly relates to OCS's students, including education records as defined in the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. §1232g and other applicable law, any personally identifiable information ("PII") about students, and any aggregated or de-identified data about OCS's students. Unless specifically provided otherwise herein, any restrictions, limitations, or conditions regarding Provider's use of OCS Data apply equally to Provider's use of Student Data or Confidential Student Data.

   d. "**Confidential Student Data**." "Confidential Student Data" is a subset of "Student Data." "Confidential Student Data" includes education records as defined in the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. §1232g and other applicable law, any personally identifiable information ("PII") about students, but not any aggregated or de-identified data about students that would not, when considered in isolation or in conjunction with other reasonably available information, allow a reasonable person in the school community to discern the identity of individual student. Unless specifically provided otherwise herein, any restrictions, limitations, or conditions regarding Provider's use of OCS Data or Student Data apply equally to Provider's use of Confidential Student Data

2. **Authorized Use of OCS Data.** OCS Data will be used by Provider solely for the purpose of providing the Services. When OCS Data includes Confidential Student Data, Provider agrees such use will be limited to institutional functions of OCS that could otherwise be provided by a school official and which OCS is "outsourcing" to Provider pursuant to 34 CFR 99.31(a)(1)(B). Provider agrees that OCS Data and all

rights to OCS Data shall remain the exclusive property of OCS, and Provider has a limited, nonexclusive, license to use such OCS Data solely for the purpose of providing such Services.

3. **Compliance with Applicable Laws, Policies, and Procedures**. Provider shall comply with all federal, state, and local laws and OCS policies that are applicable to the provision of Services hereunder, including but not limited to all applicable OCS policies regarding Confidential Student Data. Provider acknowledges that it may access the applicable OCS policies online at https://www.boardpolicyonline.com/bl/?b=orange_county_nc or by contacting OCS's central administrative office. Regarding Confidential Student Data, Provider specifically agrees to comply with the provisions of FERPA, PPRA, COPPA, and all other applicable laws and regulations in all respects, as well as any state law and applicable OCS policies. For purposes of this Agreement, FERPA includes 20 U.S.C. 1232g, Part 99 of Title 34 of the Code of Federal Regulations; PPRA includes 20 U.S.C 1232h, Part 98 of Title 34 of the Code of Federal Regulations; and COPPA includes 5 U.S.C. 6501-6505, Part 312 of Title 16 of the Code of Federal Regulations. Nothing in this Agreement shall be construed to allow Provider to maintain, use, or disclose any OCS Data in a manner inconsistent with any applicable law, regulation, or policy.

4. **Procedures for the Maintenance and Security of OCS Data**. While in the possession, custody, or control of Provider, all OCS Data shall be stored in a secure environment with access limited to the least number of employees needed to provide the Services. Provider shall develop, implement, maintain, and use appropriate administrative, technical, and physical security measures to preserve the confidentiality, integrity, security, and availability of all OCS Data. Such measures shall include processes for transmission and storage of such data.

    a. **OCS Data**. Provider shall protect OCS Data from loss, destruction, unauthorized physical and electronic access, and unauthorized uses or disclosures in accordance with commercially reasonable standards and no less rigorously than it protects its own confidential information. All OCS Data shall be kept in a secure location preventing access by unauthorized individuals. Provider agrees to handle any and all OCS Data using appropriate access control and security, including password-protection and encryption in transport and electronic storage, and periodic auditing of data at rest. Provider will conduct periodic risk assessments and remediate any identified security vulnerabilities in a timely manner.

    b. **Student Data**. Provider shall not forward to any person or entity other than OCS any Student Data except as expressly authorized in this Agreement without the advance written consent of OCS. Provider shall designate one or more individuals as the primary data custodian(s) of the Student Data and shall notify OCS of the name(s) and title(s) of such individual(s) prior to any such data being shared. The primary data custodian(s) shall ensure that the Services shall be conducted in a manner that does not permit personal identification of OCS students by anyone other than representatives or authorized subcontractors of Provider who need such information for the purposes described in Paragraph 2 of this Agreement and shall ensure that a log is maintained of all Student Data received pursuant to this

Agreement. The provisions described above related to OCS Data also apply to Student Data.

c. **Confidential Student Data**. Provider will maintain an access log delineating the date, time, and identity of any person or entity given access to any Confidential Student Data who is not in the direct employ of Provider and the reason(s) for such access. No such access shall be granted except in compliance with the terms and conditions of this Agreement and applicable law. The primary data custodian(s) described above shall be ensure the timely destruction or return of any Confidential Student Data as required by this Agreement. Confidential Student Data shall not be emailed in plain text. The provisions described above related to OCS Data and Student Data also apply to Confidential Student Data.

5. **Prohibition on Unauthorized Use or Disclosure of OCS Data**.

a. Provider agrees to hold all OCS Data in strict confidence. Provider shall not use or disclose OCS Data except as authorized by this Agreement, as separately authorized in writing by OCS, or as required by law. Provider agrees not disclose any OCS Data in a manner that could identify any individual employee, student, or user to any other individual or entity, directly or by means of deduction.

b. Provider is prohibited from mining or scanning OCS Data for any purposes other than those agreed to in advance by this Agreement or by separate written authorization of OCS.

c. Provider shall not use any Confidential Student Data, including but not limited to student and parent names, addresses, emails addresses, or similar information, for its own commercial marketing or advertising purposes, or for the commercial marketing or advertising purposes of any third-party without the advance written consent of OCS. Provider shall not use any Confidential Student Data to advertise or market products or services to OCS employees, students, families, or to any OCS-affiliated users of the Services without the advance written consent of OCS.

d. In the event of any unauthorized use or disclosure of any OCS Data, Provider shall report the incident to OCS as promptly as possible, but no more three (3) business days after Provider learns of such use or disclosure. Such report shall identify:

i. The nature of the unauthorized use or disclosure,
ii. The data used or disclosed,
iii. Who made the unauthorized use or received the unauthorized disclosure,
iv. What Provider has done and shall do to mitigate the effects of the unauthorized use or disclosure, and
v. What corrective action Provider has taken or shall take to prevent future similar unauthorized use or disclosure.

Provider shall also provide such other information related to the unauthorized use or disclosure that may be reasonably requested by OCS. OCS also may require that Provider promptly provide a written notice of the breach or disclosure, as well as a

description of the corrective actions taken, to any OCS employee, student, or user directly impacted by the breach or disclosure. Any such notice shall be subject to prior review and approval by OCS.

e. Provider may use de-identified, aggregated OCS Data, including de-identified, aggregated Student Data, for product development and research purposes. Any such de-identified data will have all direct and indirect personal identifiers removed, including but not limited to names, ID numbers, dates of birth, home addresses, phone numbers, email addresses, and similar information. Provider agrees not to attempt to re-identify any de-identified Student Data and not to transfer de-identified Student Data to any other party except as specifically authorized in this Agreement or with OCS's advance written consent. Provider will not release any research or publications pertaining to Student Data that in any way identifies OCS as the source of such data without OCS's advance written consent.

6. **Subcontractors**. Provider may share Student Data with its subcontractors only for purposes of providing the Services or with the advance written permission of OCS. Any such request from Provider shall be in writing and shall identity the person(s) or entit(ies) to whom disclosures will be made and the purposes of the disclosures. For any authorized disclosure of Student Data to a subcontractor, Provider shall ensure that each approved subcontractor is contractually bound to adhere to all of the terms of this Agreement and is aware of its obligations under applicable law with respect to its possession, use, and re-disclosure of any Confidential Student Data. Nothing in this paragraph shall relieve Provider of any of its obligations under this Agreement, including its responsibilities to ensure the confidentiality and security of any OCS Data provided by OCS pursuant to this Agreement.

7. **Monitoring and Auditing**. Any OCS Data held by Provider will be made available to OCS for review and inspection upon request of OCS. Provider shall cooperate with OCS or with any other person or agency as directed by OCS, in monitoring, auditing, or investigating activities related to Provider's use and safeguarding of the OCS Data, including but not limited to allowing reasonable inspection of the data logs or security measures described in Paragraph 4 of this Agreement. Consistent with Section 132-1.2 of the North Carolina General Statutes, OCS and its auditors will maintain the confidentiality of any trade secrets of Provider that may be accessed during an audit conducted under this Agreement.

8. **Term; Post-Termination**. This Agreement takes effect upon the date of full execution and shall continue in full force and effect for so long as Provider has possession, custody, or control of any of the OCS Data. Upon the termination of the applicable subscription, contract, purchase order, agreement, memorandum of understanding, or terms of service between OCS and Provider, or upon written notice of termination of the Services by OCS, all Confidential Student Data shall, at OCS' sole option, be destroyed or returned to OCS except for data that remains in the possession of Provider only because it has been backed up for archival purposes, which data may remain archived (but not accessed) until it is deleted per Provider's policies and standard industry practice and shall remain subject to all confidentiality and data security provisions in this Agreement. No other entity, including any subcontractors of Provider, shall be authorized to continue possessing or using any Confidential Student Data following

termination without the written consent of OCS. Except as otherwise provided herein, any Confidential Student Data remaining on any computers, servers, or other devices of Provider or its employees, agents, or subcontractors, shall be permanently deleted unless OCS specifically authorizes its post-termination retention in writing. Provider shall complete such destruction or return as promptly as possible, but not more than thirty (30) days after termination of the applicable subscription, contract, purchase order, agreement or terms of service between OCS and Provider, or written notice of termination of the Services by OCS, unless OCS extends such deadline in writing. This section shall survive the expiration or earlier termination of this Agreement.

9. **Breach and Default; Indemnification; Remedies**.

   a. In the event of a material data or security breach of OCS Data while in the possession or under the control of Provider, or, if OCS determines, in its sole discretion, that any OCS Data has been mishandled or disclosed in a manner inconsistent with this Agreement, OCS may demand the immediate return or destruction of any and all of the OCS Data.

   b. Provider shall fully indemnify and hold harmless the Orange County Board of Education and its past, current and future members, agents, and employees from and against all third-party claims, actions, demands, reasonable costs, damages, losses, and/or expenses of any kind whatsoever proximately resulting from any material data breach of this Agreement or any unauthorized use or disclosure of the OCS Data by Provider or it's subcontractor(s). The parties agree that this indemnification clause is an "evidence of indebtedness" for purpose of N. C. Gen. Stat. § 6-21.2. This section shall survive the expiration or earlier termination of this Agreement.

   c. Nothing in this Agreement shall restrict OCS from seeking any other rights or remedies to which it may be entitled at law or equity for any breach or unauthorized disclosure of OCS data for which Provider may be legally liable.

10. **No Right or Entitlement to Data**. This Agreement sets out the terms and conditions under which OCS may, in its sole discretion, provide OCS Data to Provider. Nothing in this Agreement creates any right, title, or interest in Provider to receive any such information.

11. **Relationship to Service Contract**. This Security Agreement governs Provider's maintenance, use, and disclosure of OCS Data, Student Data, and/or Confidential Student in the course of providing the Services and is incorporated by reference as part of the Parties' underlying service contract. To the extent of any conflict between this Security Agreement and the service contract as they relate to Provider's maintenance, use, and disclosure of OCS Data, Student Data, and/or Confidential Student in the course of providing the Services, the terms of this Security Agreement will control.