EDUCATION LAW 2-d RIDER

New York State Education Law 2-d was enacted in 2014 to address concerns relative to securing certain personally identifiable information. In order to comply with the requirements of Education Law 2-d, educational agencies and certain third-party contractors who contract with educational agencies must take certain additional steps to secure such data. These steps include enacting and complying with a Parents' "Bill of Rights" relative to protected data, ensuring that each third-party contractor has a detailed data privacy plan in place designed to ensure the security of such data, and that each third-party contractor sign a copy of the educational agency's Parents' Bill of Rights, thereby signifying that the third-party contractor will comply with such Parents' Bill of Rights. This Agreement is subject to the requirements of Education Law 2-d and Cengage Learning, Inc. (the "Contractor") is a covered third-party contractor.

In order to comply with the mandates of Education Law 2-d, and notwithstanding any provision of the Agreement between the LINDENHURST UNION FREE SCHOOL DISTRICT (the "District") and Contractor to the contrary, Contractor agrees as follows:

Contractor will treat "Protected Data" (as defined below) as confidential and shall protect the nature of the Protected Data by using the same degree of care, but not less than a reasonable degree of care, as the Contractor uses to protect its own confidential data, so as to prevent the unauthorized dissemination or publication of Protected Data to third parties. Contractor shall not disclose Protected Data other than to those of its employees, agents, or subcontractors who have a need to know such Protected Data under this Agreement, or as otherwise permitted by this Agreement or required by law. Contractor shall not use Protected Data for any other purposes than to provide services under the Agreement, as required by law, or as explicitly provided for in this Agreement. All Protected Data shall remain the property of the disclosing party. As more fully discussed below, Contractor shall have in place reasonable internal controls designed to ensure that the District's Protected Data is safeguarded in accordance with all applicable laws and regulations, including, but not limited to, the Children's Internet Protection Act ("CIPA"), the Family Educational Rights and Privacy Act ("FERPA"), the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and Part 121 of the Regulations of the Commissioner of Education, as it may be amended from time-to-time if applicable.

"**Protected Data**" includes any information rendered confidential by applicable State or federal law, including, but not limited to student data, student demographics, scheduling, attendance, grades, health and discipline tracking, and all other data reasonably considered to be sensitive or confidential data by the District and designated to Contractor as such. Protected Data also includes any information protected under Education Law 2-d including, but not limited to:

> "Personally identifiable information" from student records of the District as that term is defined in § 99.3 of FERPA,

-AND-

Personally identifiable information from the records of the District relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§3012-c and 3012-d.

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any Protected Data shall comply with New York State Education Law § 2-d. As applicable, Contractor agrees to comply with District policy(ies) on data security and privacy. Contractor shall promptly reimburse the District for all reasonable, documented costs of notifying a parent, eligible student, teacher, or principal of an unauthorized release of Protected Data by Contractor, its subcontractors, and/or assignees caused by Contractor, its subcontractors, and/or assignees. In the event this Agreement expires, is not renewed or is terminated, Contractor shall return or delete all of the District's data unless otherwise provided, including any and all Protected Data, in accordance with Contractor's data retention and destruction policies. Notwithstanding the foregoing, Contractor may retain Protected Data for the purposes of complying with law, provided that the terms of this Agreement shall survive and apply with respect to such Protected Data and Contractor shall only use and disclose the retained Protected Data for the purposes that require its retention.

Data Security and Privacy Plan

Contractor shall maintain a Data Security and Privacy Plan which includes the following elements:

1. Specifies the administrative, operational and technical safeguards and practices in place to protect personally identifiable information that Contractor will receive under the contract;

2. Demonstrates Contractor's compliance with the requirements of Section 121.3 of Part 121;

3. Specifies how officers or employees of the Contractor and its assignees who have access to student data, or teacher or principal data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;

4. Specifies how Contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;

5. Specifies how Contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the educational agency;

6. Specifies whether Protected Data will be returned to the District, transitioned to a successor contractor, at the District's option and direction, deleted or destroyed by the Contractor when the contract is terminated or expires.

Initial Here: Pursuant to the Plan Contractor will:

1. Have adopted reasonable technologies, safeguards and practices that align with the NIST Cybersecurity Framework referred to in Part 121.5(a);

CS

CS

CS

2. Comply with the data security and privacy policy of the District; Education Law § 2-d; and Part 121;

3. Have limited internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services;

Initial Here:

CS 4. Have prohibited the use of personally identifiable information for any purpose not explicitly authorized in this contract;

CS 5. Have prohibited the disclosure of personally identifiable information to any other party without the prior written consent of the parent or eligible student:

   a. except for authorized representatives such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with state and federal law, regulations and its contract with the educational agency; or

   b. unless required by statute or court order and Contractor has provided a notice of disclosure to the department, district board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.

CS 6. Maintain reasonable administrative, technical and physical safeguards designed to protect the security, confidentiality and integrity of personally identifiable information in our custody;

CS 7. Use encryption designed to protect personally identifiable information in its custody while in motion or at rest; and

CS 8. Not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

In the event Contractor engages a subcontractor to perform its contractual obligations and before disclosing Protected Data, Contractor agrees to impose by written contract data protection obligations not materially less protective than those imposed on the Contractor by state and federal law and this Agreement.

Where a parent or eligible student requests a service or product from a Contractor and provides express consent to the use or disclosure of personally identifiable information by Contractor for purposes of providing the requested product or service, such use by Contractor shall not be deemed a marketing or commercial purpose prohibited by the Plan.

Contractor's signature below shall also constitute an acknowledgement, acceptance, and signature of the District's Parent Bill of Rights.

NOTWITHSTANDING ANYTHING IN THIS AGREEMENT TO THE CONTRARY, AND EXCEPT FOR GROSS NEGLIGENCE AND DELIBERATE MISCONDUCT, CONTRACTOR'S CUMULATIVE LIABILITY ARISING OUT OF OR RELATED TO THIS

AGREEMENT SHALL NOT EXCEED THE ACTUAL COSTS INCURRED BY THE DISTRICT IN ORDER TO REMEDY ANY BREACH OF THE OBLIGATIONS HEREUNDER, AND IN NO EVENT, SHALL THE CONTRACTOR'S CUMULATIVE LIABILITY EXCEED THE TOTAL AMOUNT OF TWO HUNDRED AND FIFTY THOUSAND DOLLARS ($250,000.00). IN NO EVENT, OTHER THAN CASES OF GROSS NEGLIGENCE AND/OR DELIBERATE MISCONDUCT, SHALL CONTRACTOR BE LIABLE TO THE DISTRICT IN ANY RESPECT, FOR PUNITIVE DAMAGES, ARISING OUT OF THIS AGREEMENT OR THE ACTS OR OMISSIONS IN FULFILLING ITS OBLIGATIONS HEREUNDER.

NAME OF PROVIDER:_Cengage Learning, Inc._____

SIGNED BY: Cynthia Scheffer _____ **DATED:** 1/30/25

TITLE: Sr. Sales Director, Milady

DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN IS ATTACHED HERETO AND INCORPORATED HEREIN.

(1) Specifies the administrative, operational and technical safeguards and practices in place to protect personally identifiable information that Contractor will receive under the contract;

a. Administrative:

i. Contractor implements, maintains, and periodically updates privacy and information security policies and procedures designed to address compliance with privacy and security requirements that are both regulatory and contractual in nature.

ii. Contractor has dedicated privacy and security personnel responsible for implementing, maintaining, and managing its privacy and security compliance programs.

iii. Contractor security and privacy personnel are involved in the contract negotiation process in a manner designed to ensure that Contractor can comply with agreed-to contractual obligations.

iv. Contractor conducts periodic internal risk assessments to identify the risks to District data pursuant to NIST frameworks. These risk assessments include a review of internal, external, and third-party risks and include within their scope review of subcontractor agreements and subcontractor privacy and security audit reports. Material identified risks and gaps are remediated or mitigated through updated controls, safeguards, configurations, or other compensating or mitigating measures.

v. Contractor conducts periodic technical risk and vulnerability assessments using third-party scanning and assessment tools, penetration/vulnerability testing for Contractor hosted solutions, and review of security audit reports for subcontractors.

vi. Contractor utilizes appropriate administrative controls which includes privacy, security, and corruption awareness trainings; documented IT and security policies; an Incident Response Plan; facility access controls; onboarding controls including background checks; vendor risk assessments; IT procurement policies; Business continuity and DR policy, etc.

b. Operational:

i. Contractor has developed and maintains industry appropriate operational controls including: password management and access management policies and procedures based on the principle of least privilege; a documented change management process; Software Development Life Cycle policies and procedures; patching and maintenance policies and procedures; and periodic security program risk assessments designed to identify risks to the privacy and security of customer data. Assessments are conducted by a dedicated in-house security team using third-party scanning and assessment tools and third-party penetration and vulnerability reviews, are conducted pursuant to NIST 800-53

risk control evaluations, and risks are tracked and escalated using a ServiceNow risk register.

c. Technical:
    i. Contractor utilizes third-party tools for intrusion detection, antivirus/antimalware, web application firewall and other firewall protections, identity safeguards with single sign-on and multi-factor authentication, virtual private network technologies for remote access, Cloud Infrastructure as a Service protection technologies and configurations, advanced logging and Security Information and Event Management, IaaS toolsets, and third party enterprise class technical suites.

(2) Specifies how officers or employees of the Contractor and its assignees who have access to student data, or teacher or principal data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;

a. Contractor provides privacy and security awareness training courses for its employees as well as compliance and anti-corruption training upon hire and no less often than annually, in each case provided to its employees by an online learning management system (LMS) with recording of completion tracked by the LMS.

(3) Specifies how Contractor will utilize subcontractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;

a. Contractor uses subcontractors in connection with the services to be provided hereunder, including cloud hosting services, call center services, e-commerce platform and payment services, and also develops APIs with major LMS providers that often allow delivery of Contractor content through existing customer software implementations.
b. Contractor engages subcontractors pursuant to the following controls:
    i. Contractor conducts pre-engagement due diligence on subcontractors regarding privacy and security protections;
    ii. Subcontractors are required to agree to written agreements containing privacy and security terms that protect customer information consistent with the requirements of applicable law;
    iii. Contractor periodically reviews audit reports and assessments conducted by its sub-contractors regarding security controls; and
    iv. Contractor conducts periodic audits and reviews of sub-contractors where it deems necessary consistent with its vendor management policies.

(4) Specifies how Contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the educational agency;

a. Contractor has a formally documented incident response plan covering both privacy and security incidents, which includes appropriate management and notification details and review of contracts with impacted customers in a manner designed to ensure timely notification within the timeframes designated in customer contracts and required by law.

(5) Specifies whether Protected Data will be returned to the District, transitioned to a successor contractor, at the District's option and direction, deleted or destroyed by the Contractor when the contract is terminated or expires..

a. Contractor securely deletes data within sixty (60) days of termination, or if an earlier time is requested in writing by the District, it will use commercially reasonable efforts to meet such timeline, in each case in a manner consistent with NIST and industry standard secure deletion and destruction mechanisms.