SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION

As per the Agreement between the undersigned and Nassau BOCES, this information must be completed by the Service Provider within ten (10) days of execution of the Agreement.

Name of Provider:	Instructure. Inc.
Description of the purpose(s) for which Provider will receive/access PII:	Please see attached "Instructure Elevate Services - NY 2D Data Security and Privacy Plan". Instructure will only use customer data to provide the services purchased by the customer.
Type of PII that Provider will receive/access:	Check all that apply: ☑ Student PII ☑ APPR Data
Contract Term:	Contract Start Date: _____ Contract End Date: _____
Subcontractor Written Agreement Requirement:	Provider will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by State and Federal laws and regulations, and the Contract. (check applicable option) ☐ Provider will not utilize subcontractors. ☑ Provider will utilize subcontractors.
Data Transition and Secure Destruction:	Upon expiration or termination of the Contract, Provider shall: • Securely transfer data to Nassau BOCES, or a successor provider at Nassau BOCES' option and written discretion, in a format agreed to by the parties. • Securely delete and destroy data.
Challenges to Data Accuracy:	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting Nassau BOCES. If a correction to data is deemed necessary, Nassau BOCES will notify Provider. Provider agrees to facilitate such corrections within 21 days of receiving Nassau BOCES' written request.

Secure Storage and Data Security:	Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply) ☑ Using a cloud or infrastructure owned and hosted by a third party. ☐ Using Contractor owned and hosted solution. ☐ Other: Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data: Please see section 6.0 of the attached "Instructure Elevate Services - NY 2[
Encryption :	Data will be encrypted while in motion and at rest.

PROVIDER	
[Signature]	Daisy Bennett
[Printed Name]	Daisy Bennett
[Title]	AGC
Date:	May 17, 2024

Instructure Elevate Services - NY 2D Data Security and Privacy Plan

April 2024

Table of Contents

1.0 Purpose

The purpose of this Instructure Elevate Services NY 2D Data Security and Privacy Plan (the "Plan") is to document Instructure Inc.'s commitment and approach to protecting Confidential Information (as defined in Section 2.0 below), and how it will handle any incidents where there is a breach or unintended disclosure of Confidential Information or a System (as defined in Section 2.0 below) that supports it. This Plan applies specifically to the Elevate Services offered by Instructure..

2.0 Terminology

Application(s) – means Instructure's commercially offered software that performs a user-facing function, such as a web application.

Confidential Information or Data – means any personally identifiable information related to students, student families/guardians, local education agency (LEA) employees, agents and/or volunteers obtained by or furnished to Instructure; all findings, analysis, data, reports or other information learned or developed and based thereon, whether in oral, written, graphic, or machine-readable form; and all information marked "confidential" by the LEA.

Confidential Information includes names, addresses, contact information, school or school attended, school district, grades or other reviews, credits, scores, analysis or evaluations, records, correspondence, activities or associations, financial information, social security numbers or other identifying numbers or codes, date of birth or age, gender, religion, sexual preference, national origin, socio-economic status (including free/reduced lunch status), race, ethnicity, special education status, or English Language Learner status, and any other information that constitutes "personally identifiable information" as defined in or pursuant to the Family Educational Rights and Privacy Act (20 U.S.C. 1232g and 34 C.F.R. Part 99) (collectively, "FERPA"), or "personally identifying information" as defined or used in New York Education Law 3012-c.

Confidential Information does not include any information that is: (i) lawfully in the public domain at the time of receipt or which lawfully comes into the public domain thereafter through no act of Instructure, (ii) demonstrated to have been known to the Instructure prior to disclosure by or through the LEA, (iii) disclosed with the prior written approval of the LEA, (iv) demonstrated to have been independently developed by the Instructure without reference to the Confidential Information, (v) disclosed to Instructure by a third party under conditions permitting such disclosure, and/or (vi) disclosed as required by court order, subpoena, other validly issued administrative or judicial notice or order and/or as a matter of applicable law; provided.

Notwithstanding the previous sentence, "personally identifiable information" as defined or used in FERPA or New York Education Law Section 2d, or "personally identifying information" as defined or used in New York Education Law §3012-c remains Confidential Information notwithstanding (A) the applicability of items (i), (ii), (iii) and (vi) in the previous sentence, and (B) items (iv) and (v) of the previous sentence to the extent that such disclosures were made at the direction of or such information was maintained on behalf of the LEA.

Data Controller – The individual or legal entity which controls the contents and use of PII.

FERPA – means the Family and Educational Rights and Privacy Act (20 U.S.C. 1232g) and any applicable regulations promulgated thereunder, including but not limited to 34 C.F.R. Part 99.

Handle –means (in the context of Confidential Information) to create, view, modify, store, transmit or delete.

Local Education Agency (LEA) – means a school district or an educational service agency.

PII – means personally identifiable information, as defined under FERPA.

System – means any information technology processing device, including routers, servers, Applications, workstations and mobile devices.

Instructure – means Instructure Elevate Solutions.

3.0 Relevant Laws, Regulation, Policies and Standards

3.1 Family Education Rights and Privacy Act (FERPA)

FERPA is the primary federal legislation that governs the privacy of educational records. Instructure holds all PII obtained, learned or developed by Instructure in confidence pursuant to applicable provisions of FERPA. Instructure understands that under FERPA it must limit access to PII to those who need to know the information for Instructure to perform its duties under an applicable contract, and to destroy all copies of PII, or to return PII to the LEA, when no longer needed or at the expiration of any contract. Instructure understands that upon request, it must permit the LEA access to PII that it holds, for the LEA to meet other obligations under FERPA or pursuant to law.

3.2 New York Education Law § 3012-c(10)

New York Education Law § 3012-c(10) governs the confidentiality of certain Confidential Information concerning teacher and principal evaluation data. Instructure understands that to the extent that information protected under New York State Education Law §3012-c(10) is shared with Instructure, Instructure is responsible for complying with the applicable provisions of this law. Instructure further understands that New York State Education Law § 2-d imposes additional requirements concerning such Confidential Information.

3.3 New York State Education Law § 2-d

New York State Education Law §2-d is a state law that imposes a number of confidentiality and data security requirements in addition to those found in FERPA and New York Education Law §3012-c(10), including a number of requirements and obligations that apply directly to Instructure. Instructure understands that it is required to comply with the applicable requirements of New York Education Law 2-d and any regulations promulgated thereunder. Instructure understands that among other requirements, New York Education Law §2-d requires Instructure to:

- Limit internal access to Confidential Information covered under Education Law §2-d (“Covered Confidential Information”) to those with legitimate educational interests;
- Not use Covered Confidential Information for any other purposes than those authorized in any contract to which it is party;

- Not disclose Covered Confidential Information without parental consent, except to authorized representatives of Instructure who are carrying out any contract it is party to;
- Maintain reasonable technical, administrative and physical safeguards to protect Covered Confidential Information;
- Not sell covered Confidential Information, nor use Covered Confidential Information for marketing purposes;
- Provide training on laws governing confidentiality to its officers, employees and assignees with access to Covered Confidential Information;
- Use encryption technology to protect Covered Confidential Information while in motion or in its custody from unauthorized disclosure, using a technology or methodology specified under HIPAA by the US Department of Health and Human Services; and
- Notify the LEA of any security breach resulting in an unauthorized release of Covered Confidential Information, and to promptly reimburse LEA for the full notification cost.

Instructure also agrees to cooperate with the LEA in complying with any applicable regulations implementing New York Education Law § 2-d and any applicable state policies promulgated pursuant to New York Education Law § 2-d, including but not limited to any requirements concerning (a) the inclusion of a data security and privacy plan in Instructure's contract with the LEA, (b) its compliance with any future state data privacy/security policy, (c) its compliance with and signature of the Parents' Bill of Rights required of the LEA, and (d) the inclusion of supplemental information concerning Instructure's contract in the Parents' Bill of Rights.

4.0 Data Accuracy, Privacy and Protection

4.1. Data Accuracy

In accordance with the applicable provisions of the regulations in Section 3.0 of this Plan, Instructure will take all reasonable steps to ensure the Confidential Information it processes is accurate, and complete. Should there be a challenge to the accuracy of this data:

A. A request to Instructure should be made in writing;

B. Within a reasonable amount of time, Instructure will determine if the request is consistent with its own assessment of the accuracy of the Confidential Information; and

C. If it is determined that the Confidential Information is inaccurate, Instructure will take the necessary steps to correct, or instruct the LEA to correct said inaccuracy and to inform the requestor, accordingly.

4.2 Privacy and Confidentiality

Instructure will:

A. Comply with all of the applicable provisions laws, regulation, policies and standards listed in Section 3.0 of this Plan;

B. Hold Confidential Information in strict confidence, limit internal access to it to those individuals who have a legitimate educational interest in such records (via administrative processes and Application and System authentication mechanisms);

C. Not disclose Confidential Information to any third parties nor make use of such Confidential Information for its own benefit or for the benefit of another, or for any use other than the purpose agreed upon with the LEA and established by the Parents' Bill of Rights in the case of New York State Education Law § 2-d;

D. Provide training on federal and state law governing Confidential Information to any officers, employees, or assignees prior to them having access to Confidential Information; and

E. Ensure Confidential Information will not appear in URLs of any Application.

4.2.1 Statement of Use

Instructure will adhere to the following principles regarding the use of Confidential Information:

A. Use Confidential Information only to the extent necessary per the purpose agreed upon with the LEA and established by the Parents' Bill of Rights in the case of New York State Education Law § 2-d;

B. Confidential Information will not be used for marketing purposes or in any manner other than what is agreed upon with the LEA and established per the laws and regulations identified in Section 3.0 of this Plan; and

C. Acknowledge the LEA as the Data Controller.

4.3 Data Security and Physical Safeguards

Instructure has implemented the following internal controls and physical safeguards:

A. Application hardware housing and/or processing Confidential Information are in a secured environment;

B. Commercially reasonable efforts are in place to keep Applications separate from general systems and applications;

C. Controlled access to Instructure's operations; only authorized individuals may enter the physical site where the Instructure's Applications are hosted;

D. Only individuals approved by Instructure may access Applications storing or transmitting Confidential Information;

E. Protect and secure all Confidential Information in transit (collected, copied and moved) and at rest (stored on the physical servers), including during any electronic data transmission or electronic or physical media transfer;

F. Maintains all copies or reproductions of Confidential Information with the same security it maintains the originals, and at the point in which the Confidential Information is no longer useful for its primary or retention purposes, as specified by the LEA, will destroy such Data, making it unusable and unrecoverable; and

G. Use commercially reasonable efforts to secure and defend any System housing Confidential Information against third parties who may seek to breach the security thereof, including, but not limited to breaches by unauthorized access or making unauthorized modifications to such System, that will involve at least the following best practice technology approaches:

    i. Authentication (i.e., passwords);

    ii. Encryption;

iii. Firewalls – hardware and software.

5.0 Incident Response Plan

In the unlikely event an incident occurs where there is a breach or unintended disclosure of Confidential Information or a System that supports it, Instructure will adhere to this Incident Response Plan.

A. Instructure will comply with all applicable breach notification laws, including New York State Education Law § 2-d and the New York State Data Breach Notification Act (General Business Law §899-aa and New York State Technology Law § 208, as appropriate).

B. Instructure will notify the LEA in writing without unreasonable delay of a breach or unintended disclosure of Confidential Information or a System that supports it.

C. Response actions to incidents that might affect Confidential Information or Systems will be conducted quickly and with ample resources. Instructure will hire a professional third-party incident response team if in-house resources do not have sufficient skill or availability.

D. Instructure will provide the LEA with the opportunity to view all incident response evidence, reports, communications and related materials, if they so request.

E. If requested by the LEA, or if required by law, Instructure will notify in writing all persons affected by the incident, at its own cost and expense.

6.0 Subcontractors

If Instructure utilizes subcontractors to support a System that Handles Confidential Information, such subcontractors are subject to, and Instructure contractually requires that each subcontractor complies with obligations substantially similar to the requirements set forth herein.