Docusign Envelope ID: 2CA2C64F-DDB7-4071-8C9C-F1D2380724BA

Addendum "A"

DATA PRIVACY PLAN AND PARENTS' BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY

Pursuant to Section 2-d of the Education Law, agreements entered between the District and a third-party contractor which require the disclosure of student data and/or teacher or principal data that contains personally identifiable information ("PII") to the contractor, must include a data security and privacy plan and must ensure that all contracts with third-party contractors incorporate the District's Parents' Bill of Rights for Data Security and Privacy. Available here: https://www.ithacacityschools.org/tfiles/folder240/parents-bill-of-rights.pdf

As such, **Littera Education, Inc** agrees that the following terms shall be incorporated into the contract for services ("the Contract") and it shall adhere to the following:

1. The Contractor's storage, use and transmission of student and teacher/principal PII shall be consistent with the District's Data Security and Privacy Policy available here: [ICSD Policy on Data Security and Privacy]

2. Contractor shall not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or permit another party to do so.

3. The exclusive purposes for which the student data or teacher or principal data will be used under the contract are set forth in Section 7 of the Contract only for the term of the Contract as set forth in Paragraph 1.

4. The Contract shall maintain the following administrative, operational and technical safeguards and practices in place to protect PII, which shall align with the NIST Cybersecurity Framework, including:

    a. PII data will be protected using encryption while in motion and at rest by

    All data is always encrypted and secured while in flight and at rest. Data in flight is encrypted using 1.2 TLS or better. Data at rest is encrypted using AWS's EBS volume XTS-AES-256 cipher.

    b. PII will be stored in a manner as to protect its security and to mitigate any potential security risks. Specifically, all student data and/or teacher or principal data will be stored by *[encrypting any data at rest using AES 256 as well as using managed access to that data by using RBAC to minimize exposure]*. The security of this data will be ensured by *[using AWS Cloud services, Daily security scans, Ai automated Penn Tests, and annual 3rd party human driven Penn Tests.]*. Littera will carry out responsible stewardship and appropriate use of Student PII in adherence to CIPA, COPPA, FERPA, and all other laws applicable to us as School Service Providers.

Docusign Envelope ID: 2CA2C64F-DDB7-4071-8C9C-F1D2380724BA

c. Physical access to PII by individuals or entities described in paragraph 3 above shall be controlled as follows:

All employees and contractors are required to follow Littera's Data Management and Password Management policies (said policies can be provided upon request). Access to software is provisioned by the application owner, based on the principle of least privilege. All employees that separate from Littera go through an offboarding process where all of their access to Littera systems, including any customer data, is removed. Any temporary access is determined and logged in the respective vendor agreement. System access is limited to the dates of the agreement.

All confidential information is encrypted in transit and at rest using algorithms and key lengths consistent with the most recent NIST guidelines. All operating systems, servers, and network devices that support confidential information are kept hardened and patched. Littera employs automated scanning and reporting mechanisms that can be used to identify possible information security vulnerabilities and incidents. All users must report any system vulnerability, incident, or event pointing to a possible incident to the Security Incident Response Team as quickly as possible but no later than 24 hours. Littera's Security Incident Response Policy is focused on establishing controls to ensure detection of security vulnerabilities and incidents, as well as quick reaction and response to security breaches (said policy can be provided upon request).

5. The Contractor shall ensure that no PII is disclosed to employees, subcontractors, or other persons or entities unless they have a legitimate educational interest and only for purposes necessary to provide services under the Contract.

By initialing here DS JS Contractor represents that it will not utilize any subcontractors or outside entities to provide services under the Contract and shall not disclose any PII other than as required pursuant to paragraph 6 below.

6. Contractor shall ensure that all employees, subcontractors, or other persons or entities who have access to PII will abide by all applicable data protection and security requirements, including, but not limited to those outlined in applicable laws and regulations (e.g., FERPA, Education Law Section 2-d). Contractor shall provide training to any employees, subcontractors, or other persons or entities to whom it discloses PII as follows: All employees and contractors are required to follow Littera's Data Management and Password Management policies (said policies can be provided upon request). Access to software is provisioned by the application owner, based on the principle of least privilege. All employees that separate from Littera go through an offboarding process where all of their access to Littera systems, including any customer data, is removed. Any temporary access is determined and logged in the respective vendor agreement. System access is limited to the dates of the agreement.

All confidential information is encrypted in transit and at rest using algorithms and key lengths consistent with the most recent NIST guidelines. All operating systems,

Docusign Envelope ID: 2CA2C64F-DDB7-4071-8C9C-F1D2380724BA

servers, and network devices that support confidential information are kept hardened and patched. Littera employs automated scanning and reporting mechanisms that can be used to identify possible information security vulnerabilities and incidents. All users must report any system vulnerability, incident, or event pointing to a possible incident to the Security Incident Response Team as quickly as possible but no later than 24 hours. Littera's Security Incident Response Policy is focused on establishing controls to ensure detection of security vulnerabilities and incidents, as well as quick reaction and response to security breaches (said policy can be provided upon request).

7. Contractor shall not disclose PII to any other party other than those set forth in paragraph 4 above without prior written parental consent or unless required by law or court order. If disclosure of PII is required by law or court order, the Contractor shall notify the New York State Education Department and the District no later than the time the PII is disclosed unless such notice is expressly prohibited by law or the court order.

8. Upon expiration of the contract, the PII will be returned to the District and/or destroyed. Specifically, All of the district's data shall be available to the district at no additional cost and, upon request or at the end of the contract term, Littera will return the data to the district in a readily accessible electronic format, such as a CSV file.

9. The parent, student, eligible student, teacher, or principal may challenge the accuracy of the student data or teacher or principal data collected in accordance with the procedures set forth in the FERPA regulations at 99 C.F.R. Part 34, Subpart C, §§99.20-99.22.

10. The Contractor shall take the following steps to identify breaches or unauthorized releases of PII and to notify the District upon learning of an unauthorized release of PII.

    a. Provide prompt notification to the District no later than seven (7) calendar days from date of discovery of a breach or unauthorized release of PII. Contractor shall provide notification to the District's data privacy officer by phone and by email.

    b. Contractor shall cooperate with the District and law enforcement to protect the integrity of the investigation of any breach or unauthorized release of PII.

    c. Where a breach or unauthorized release is attributed to the Contractor, the Contractor shall pay for or promptly reimburse the District for the full cost of such notification.

11. A complete list of all student data elements collected by the State is available for public review at https://www.nysed.gov/sites/default/files/programs/data-privacy-security/inventory-of-data-elements-collected-by-nysed_0.pdf, or parents may obtain a copy of this list by writing

Docusign Envelope ID: 2CA2C64F-DDB7-4071-8C9C-F1D2380724BA

to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, NY 12234.

12. Parents have the right to file complaints with the District about possible privacy breaches of student data by the District's third-party contractors or their employees, officers, or assignees, or with NYSED. Direct complaints to:

    Zach Lind - Assistant Superintendent
    Ithaca City School District
    602 Hancock Street
    Ithaca, NY 14850
    Zach.lind@icsd.k12.ny.us
    607-274-2311

    Complaints to NYSED should be directed in writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany NY 12234, email to CPO@mail.nysed.gov.

The District shall publish this contract addendum on its website.

Ithaca City School District
Zach Lind, Assistant Superintendent

Littera Education, Inc

DocuSigned by:
Justin Serrano
EECF1BD16D3C465...

Justin Serrano
CEO
8/21/2025