Attachment A

PARENTS' BILL OF RIGHTS FOR STUDENT DATA PRIVACY AND SECURITY

The East Rockaway Union Free School District, in recognition of the risk of identity theft and unwarranted invasion of privacy, affirms its commitment to safeguarding student personally identifiable information in education records from unauthorized access or disclosure in accordance with State and federal law, and establishes the following parental bill of rights:

1. Students' personally identifiable information will be collected and disclosed only as necessary to achieve educational purposes in accordance with State and federal Law;

2. A student's personally identifiable information cannot be sold or released for any marketing or commercial purposes by the district or any a third party contractor. The district will not sell student personally identifiable information and will not release it for marketing or commercial purposes, other than directory information released by the district in accordance with district policy;

3. Parents have the right to inspect and review the complete contents of their child's education record;

4. State and federal laws, such as NYS Education Law §2-d and the Family Educational Rights and Privacy Act, protect the confidentiality of students' personally identifiable information. Safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred;

5. A complete list of all student data elements collected by the State Education Department is available for public review at http://nysed.gov.data-privacy-security or by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234;

6. Parents have the right to have complaints about possible breaches and unauthorized disclosures of student data addressed. Complaints should be directed to Bonnie McClelland, Director of Technology and Learning Analytics, bmcclelland@eastrockawayschools.org, 443 Ocean Avenue, East Rockaway, NY 11518, 516-887-8300, X466. Complaints can also be directed to the New York State Education Department online at http://nysed.gov.data-privacy-security, by mail to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234 or by email to privacy@mail.nysed.gov or by telephone at 5178-474-0937;

7. Parents have the right to be notified in accordance with applicable laws and regulations if a breach or unauthorized release of their student's personally identifiable information occurs;

8. Parents can expect that educational agency workers who handle personally identifiable information will receive annual training on applicable federal and state laws, regulations, educational agency's policies and safeguards which will be in alignment with industry standards and best practices to protect personally identifiable information;

9. In the event that the District engages a third party provider to provide, deliver or facilitate student educational services, the contractor or subcontractors will be obligated to adhere to the District's data security and privacy policy and with State and federal laws to safeguard students' personally identifiable information, as well as to this Bill of Rights and required supplemental information for each contract.

10. This Parents' Bill of Rights will be included with every contract or other written agreement entered into by the District with a third-party contractor if the contractor will receive student data or teacher or principal data. The Bill of Rights shall also be supplemented to include information about each contract or other written agreement that the District enters into with a third-party contractor receiving student data or teacher or principal data, including: the exclusive purpose(s) for which PII Data will be used; how the contractor will ensure confidentiality and data protection and security requirements; the duration and date of expiration of the contract and what happens to PII Data upon the expiration of the contract; if and how the accuracy of PII Data collected can be challenged; where the student data or teacher or principal data will be stored, described in such a manner as to protect data security, and the security protections taken to ensure such data will be protected and data security and privacy risks mitigated; and how PII Data will be protected using encryption while in motion and at rest.

11. Parents can request information about third party contractors by contacting Bonnie McClelland, Director of Technology and Learning Analytics, bmcclelland@eastrockawayschools.org, 443 Ocean Avenue, East Rockaway, NY 11518, 516-887-8300 X466 or can access the information on the district's website *https://eastrockawayschools.org/*

12. This Parents' Bill of Rights and supplemental information for contracts with third-party contractors shall be posted on the District's website at: *https://eastrockawayschools.org/departments/technology*

* * *

PARENTS' BILL OF RIGHTS FOR STUDENT DATA PRIVACY AND SECURITY THIRD PARTY CONTRACTOR SUPPLEMENT

In accordance with its obligations under the District's Parents' Bill Rights and Data Privacy and Security Agreement, the Contractor verifies the following supplemental information to the Parents' Bill of Rights regarding data privacy and security:

(1) The student data or teacher or principal data (collectively, "PII Data") received by the Contractor will be used exclusively for the following purpose(s):

Contractor and its agents, employees and subcontractors, if any, shall use PII Data solely for the purpose of providing services as set forth in the parties' contract or other written agreement. Contractor and its agents, employees and subcontractors will not use PII Data for any other purposes. Any Data received by or by Contractor or any of its agents, employees, subcontractors or assignees shall not be sold or released for any commercial purposes, nor shall it be sold or used for marketing purposes.

(2) The Contractor will ensure the confidentiality of PII Data that is shared with subcontractors or other persons or entities as follows:

In the event that Contractor subcontracts with an outside entity or individual in order to fulfill its obligations to the District, Contractor ensures that it will only share PII Data with such subcontractors if those subcontractors are contractually bound to observe obligations to maintain data privacy and security consistent with those required of Contractor pursuant to the Agreement. Contractor will maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of PII Data in its custody consistent with the data protection and security requirements of district policy, and state and federal law and regulations by (*describe methods/procedures to safeguard data use by subcontractors*).

(3) The duration of Contractor's services begins on (*insert date*) and ends on (*insert date*), as set forth in the parties' contract or other written agreement. Once the contractor has completed its service to the district, records containing PII Data received by the Contractor will be disposed of as follows:

All PII Data will be disposed of in accordance with the instructions of the District, and will be: (a) delivered to the District or transitioned to a successor contractor, at the District's option and direction, (b) de-identified and/or (c) deleted from Contractor's computer systems and destroyed. Contractor will provide written confirmation of such disposition to the District, upon written request.

(4) A parent, student, teacher or principal can challenge the accuracy of PII Data received by the Contractor as follows:

In the event that a parent or eligible student wishes to challenge the accuracy of PII Data concerning that student that is maintained by Contractor or its subcontractors, such challenge may be processed through the procedures provided by the applicable educational agency or institution for amendment of education records under the Family Educational Rights and Privacy Act (FERPA). In the event that Contractor is notified of the outcome of any such errors made by Contractor, it will promptly correct any inaccurate data it or its subcontractors or assignees maintain. The District or the applicable New York education agency/institution will use FERPA's data correction procedures, as applicable, to update any data that is not a result of an error made by Contractor or its subcontractors.

(5) The following is how PII Data will be stored and what security protections will be taken by the Contractor:

All Data in Contractor's possession will be securely stored (*describe the location in a manner that protects data security*). Contractor represents that the following security protections, including encryption where applicable, will be in place to ensure that PII Data is protected. (*Describe the following, as applicable*):

- Password protections
- Administrative procedures
- Encryption while PII is in motion and at rest
- Firewalls

THIRD-PARTY CONTRACTOR'S DATA SECURITY AND PRIVACY PLAN

In accordance with its obligations under the District's Parents' Bill Rights and Data Privacy and Security Agreement, the Contractor represents and warrants that its data security and privacy plan described below or attached hereto contains the following minimum required provisions:

(i) Contractor will implement State and federal data security and privacy contract requirements for the duration of its contract that is consistent with the school district's data security and privacy policy by:

We follow relevant state & federal student privacy laws
We only collect and use data for the educational purpose described in the contract
We require confidentiality agreements for employees who handle data
We do not sell or share data for marketing or any unauthorized purpose
We would notify the district of any breach, as required by law

(ii) Contractor will use the following administrative, operational and technical safeguards to protect personally identifiable information:

We have an internal document we follow that includes Data Protection and Privacy, Platform Security, Access Control, Employee Training and Awareness, Incident Response, Third-Party and Vendor Management, and Regulatory Alignment. Ellii prioritizes customer data protection by following NIST guidelines and using robust security measures like encryption and secure passwords. Our platform employs high-standard security practices, including HTTPS and AES-256 encryption. Access to sensitive data is tightly controlled following the least privilege principle. Staff receive mandatory security training and must report any security incidents. Ellii has strict protocols for managing third-party access to data and regularly reviews its security policies to stay compliant with educational data laws. While not yet GDPR compliant, We are aware of its importance and we aim to align with similar high standards to ensure trust and privacy within the education sector.

(iii) Contractor has complied with requirements of §121.3(c) of the Commissioner's Regulations by providing and complying with the supplemental contractor information attached to its contract or written agreement with the District, or as follows:

See attached Supplemental Information form

(iv) Contractor's employees and any assignees with access to student data, or teacher or principal data have received or will receive training on relevant confidentiality laws, before receiving access to such data, as follows:

During the onboarding process, new hires complete mandatory training sessions focused on data protection laws, company privacy policies, and the handling of PII, which is followed by regular updates and refreshers. Access to PII is provisioned on a least-privilege basis, ensuring employees can only interact with the data essential for their job functions. In our offboarding procedures, access to any systems containing PII is immediately revoked when an employee's resignation or termination process begins. We conduct exit interviews to emphasize confidentiality agreements and their post-employment obligations. All company-owned devices are returned and thoroughly inspected to ensure no PII remains stored. Moreover, we maintain an audit trail of data access and alterations made by the employee to comprehensively secure and account for all PII.

(v) Contractor will use the following subcontractors and will ensure that personally identifiable information received by its subcontractors is protected, as follows:

See attached Third-Party Vendors sheet

(vi) Contractor will implement an action plan for handling any breach or unauthorized disclosure of personally identifiable information and will promptly notify the school district of any breach or unauthorized disclosure as follows:

In the event that Student Data is accessed or obtained by an unauthorized individual, Contractor shall provide notification to District within a reasonable amount of time of the incident, and not exceeding forty-eight (48) hours. Contractor shall follow the following process:
- The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described herein under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information."
Additional information may be provided as a supplement to the notice.

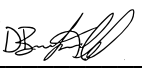
(vii) Data will be returned, transitioned to a successor contractor, deleted or destroyed when the contract ends or is terminated as follows:

Data will be deleted after 5 years of inactivity or when it's requested by the group account administrator.

EXHIBIT "B"
Contractor's Supplemental Information

Name of Contractor	Red River Press Inc. / elliii.com
Description of the purpose(s) for which Contractor will receive/access PII	To ensure the system will function properly, allowing admins to manage teachers, teachers to manage students and assignments, and students to complete assignments.
Type of PII that Contractor will receive/access	Check all that apply: ☒ Student PII ☐ APPR Data
Agreement Term	Agreement Start Date: January 12, 2026 Agreement End Date: January 12, 2027
Subcontractor Written Agreement Requirement	Contractor will not utilize subcontractors without a written agreement 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 Agreement. (check applicable option): ☐ Contractor will not utilize subcontractors. ☒ Contractor will utilize subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Contractor shall: • Securely transfer data to District, or a successor contractor at the District's 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 the District. If a correction to data is deemed necessary, the District will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the District's 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: We have implemented a comprehensive security strategy covering all aspects of data management. We encrypt all sensitive data in transit and at rest, limit access to authorized personnel, use secure hosting services, and conduct regular security audits. Our company takes data security and privacy seriously, and we are committed to ensuring that our clients' sensitive information is always protected.
Encryption	Data will be encrypted while in motion and at rest.

Contractor: Red River Press Inc. / elliii.com

Signature:  **Date:** January 12, 2026

Printed Name: Ben Buckwold **Title:** CEO

Third Party Inventory

Name	Nature	Data Shared	Location	Contact
HelpScout	Email platform; Help Docs	Name, email, any info they provide to us; communication	US	privacy@helpscout.com
Recurly	Process recurring billing	Name, email, org address, country, phone, billing information	US	privacy@recurly.com
Pipedrive	Prospect and customer relationship management	Name, email, org address, country, phone, billing information	US	privacy@pipedrive.com
PayCove	Invoicing	Name, email, org address, country, phone, billing information	US	admin@paycove.io
Customer.io	Email marketing	personal contact information	US	privacy@customer.io
Mixpanel	Data analysis	personal / education/usage data that forms the basis for the analytics	US	API for access to data: https://developers.amplitude.com/reference#ccpa-dsar-apis API to delete data: https://developers.amplitude.com/docs/user-deletion Other: privacy@amplitude.com
AWS	Cloud infrastructure	No access to data in normal course of business	US	Not applicable - no access to customer data
Heroku	Platform as a service	Data is encrypted; no access to data in normal course of business	US	Not applicable - no access to customer data
Clever	SSO for Education	Clever shares district student data with Ellii via nightly sync	US	trust@clever.com
Google Classroom	Faux integration; Ellii provides link to content and teacher shares; Link takes student to Ellii platform	No personal data is shared with Google; Link to content	n/a	n/a