

EXHIBIT A

Bill of Rights for Data Security and Privacy

Jamestown City School District

The Jamestown City School District is committed to protecting the privacy of student data and teacher and principal data. In accordance with New York Education Law §2-d and its implementing regulations, the District informs the school community of the following:

- 1) A student's personally identifiable information cannot be sold or released for any commercial purposes.
- 2) Parents have the right to inspect and review the complete contents of their child's education record.
- 3) State and federal laws protect the confidentiality of personally identifiable information, and 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.
- 4) A complete list of all student data elements collected by New York State is available for public review at <http://www.p12.nysed.gov/student-data-privacy/student-data-inventory> or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 865 EBA, 89 Washington Avenue, Albany, New York 12234.
- 5) Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to Privacy Complaint, Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be submitted using the form available at <http://www.nysed.gov/student-data-privacy/form/report-improper-disclosure>.

Supplemental Information Regarding Third-Party Contractors

In the course of complying with its obligations under the law and providing educational services to District residents, the Jamestown City School District has entered into agreements with certain third-party contractors. Pursuant to these agreements, third-party contractors may have access to "student data" and/or "teacher or principal data," as those terms are defined by law and regulation.

For each contract or other written agreement that the District enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data from the District, the following supplemental information will be included with this Bill of Rights:

- 1) The exclusive purposes for which the student data or teacher or principal data will be used by the third-party contractor, as defined in the contract;
- 2) How the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or principal data, if any, 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);

- 3) The duration of the contract, including the contract's expiration date, and a description of what will happen to the student data or teacher or principal data upon expiration of the contract or other written agreement (e.g., whether, when, and in what format it will be returned to the District, and/or whether, when, and how the data will be destroyed);
- 4) If and how a parent, student, eligible student, teacher, or principal may challenge the accuracy of the student data or teacher or principal data that is collected;
- 5) Where the student data or teacher or principal data will be stored, described in a manner as to protect data security, and the security protections taken to ensure the data will be protected and data privacy and security risks mitigated; and
- 6) Address how the data will be protected using encryption while in motion and at rest.

BY THE VENDOR:

Karim Sabuwalla

Name (Print)



Signature

Finance Manager

Title

07/28/2020

Date

BY THE DISTRICT:

Name (Print)

Signature

Title

Date

EXHIBIT A (CONTINUED)

Supplemental Information about a Master Agreement between

Jamestown City School District and Seesaw

Jamestown City School District (District) has entered into a Master Agreement with Seesaw (Vendor), which governs the availability to the District of the following products or services:

Seesaw for Schools learning management platform for learning activities, digital portfolios, student assessment, and video-response

Pursuant to the Master Agreement (which includes a Data Sharing and Confidentiality Agreement), the District may provide to Vendor, and Vendor will receive, personally identifiable information about students and/or teachers and principals that is protected by Section 2-d of the New York Education Law (“Protected Data”).

Exclusive Purposes for which Protected Data will be Used: The exclusive purpose for which Vendor is receiving Protected Data from the District is to provide the District with the functionality of the products or services listed above. Vendor will not use the Protected Data for any other purposes not explicitly authorized above or within the Master Agreement.

Oversight of Subcontractors: In the event that Vendor engages subcontractors or other authorized persons or entities to perform one or more of its obligations under the Master Agreement (including subcontracting hosting of the Protected Data to a hosting service provider), it will require those subcontractors or other authorized persons or entities to whom it will disclose the Protected Data to execute legally binding agreements acknowledging their obligation under Section 2-d of the New York Education Law to comply with all applicable data protection, privacy and security requirements required of Vendor under the Master Agreement and applicable state and federal law and regulations.

Duration of Agreement and Protected Data Upon Termination or Expiration:

- The Master Agreement commences on the date of signature.
- Within 60 days Upon expiration of the Master Agreement without renewal, or upon termination of the Master Agreement prior to its expiration, Vendor will securely delete or otherwise destroy any and all Protected Data remaining in the possession of Vendor or any of its subcontractors or other authorized

persons or entities to whom it has disclosed Protected Data. If requested by the District, Vendor will assist the District in exporting all Protected Data previously received back to the District for its own use, prior to deletion, in such formats as may be requested by the District.

- In the event the Master Agreement is assigned to a successor Vendor (to the extent authorized by the Master Agreement), the Vendor will cooperate with the District as necessary to transition Protected Data to the successor Vendor prior to deletion.
- Neither Vendor nor any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data will retain any Protected Data, copies, summaries or extracts of the Protected Data, or any de-identified Protected Data, on any storage medium whatsoever. Upon request, Vendor and/or its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data, as applicable, will provide the District with a certification from an appropriate officer that these requirements have been satisfied in full.

Challenging Accuracy of Protected Data: Parents or eligible students can challenge the accuracy of any Protected Data provided by the District to Vendor, by contacting the District regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or principals may request to challenge the accuracy of APPR data provided to Vendor by following the appeal process in the District's applicable APPR Plan.

Data Storage and Security Protections: Any Protected Data that Vendor receives will be stored on systems maintained by Vendor, or by a subcontractor under the direct control of Vendor, in a secure data center facility located within the United States. The measures that Vendor (and, if applicable, its subcontractors) will take to protect Protected Data include adoption of technologies, safeguards and practices that align with the NIST Cybersecurity Framework, and safeguards associated with industry standards and best practices including, but not limited to, disk encryption, file encryption, firewalls, and password protection.

Encryption of Protected Data: Vendor (and, if applicable, its subcontractors) will protect Protected Data in its custody from unauthorized disclosure while in motion or at rest, using a technology or methodology that complies with Section 2-d of the New York Education Law.

Addendum for New York Districts

In accordance with New York's Education Law 2-d and Parents Bill of Rights for Data Privacy and Security, Seesaw agrees that:

- (1) Seesaw will exclusively utilize the student data, teacher data, or principal data to provide account holders with the Seesaw service;
- (2) All subcontractors for Seesaw that may access personally identifiable information of students, teachers, principals or other faculty are contractually required by Seesaw to employ data privacy and security practices that provide at least a commensurate level of protection for that data as does Seesaw;
- (3) Seesaw will either delete or return, within a commercially reasonable period of time but not to exceed 60 days, all personally identifiable information upon the expiration of any agreement when requested to do so by notification from the contracting party;
- (4) Parents have the right to inspect and review the complete contents of their child's education record that is shared with or collected by Seesaw;
- (5) Seesaw maintains a publicly available list in its Privacy Policy of all student data elements collected by Seesaw;
- (6) Any parent, student, eligible student, teacher or principal may correct inaccurate student data or teacher or principal data that is collected;
- (7) Seesaw shall provide security training on all applicable state and federal laws governing confidentiality of Student Data and/or Principal or Teacher Data prior to receiving access;
- (8) Seesaw will limit internal access to education records to those individuals that are determined to have legitimate educational interests.
- (9) Seesaw will not disclose a student's personally identifiable information to any other party:
 - (i) without the prior written consent of the parent or eligible student; or
 - (ii) unless required by statute or court order and the party provides a notice of the 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 the disclosure is expressly prohibited by the statute or court order;
- (10) Seesaw complies with all applicable state and federal laws that protect the confidentiality of personally identifiable information, including New York Education Law § 2-d, and employs data security safeguards associated with industry standards and best practices, including but not

limited to, encryption, firewalls, and password protection, both when data is stored at rest or is transferred;

(11) All student data or teacher or principal data will be stored on cloud servers within the United States and protected with industry standard and best practices procedures, including encryption when stored at rest; and

(12) Seesaw will promptly address any complaints about possible breaches of student data submitted to <https://help.seesaw.me/hc/en-us/requests/new> or mailed to:

Seesaw
180 Montgomery St.
Suite 750
San Francisco, CA 94104

In the event of a breach of confidentiality, Seesaw will provide notification to the School District within forty eight (48) hours of the incident and advise it as to the nature of the breach and the steps Seesaw has taken to minimize said breach.

Seesaw

DocuSigned by:

Alison Murphy, Head of Operations

2/4/2020

Date

District

Date