

Exhibit H

EDUCATION LAW 2-d RIDER

This Exhibit H supplements the underlying Agreement to which it is attached to ensure that the underlying Agreement conforms to the requirements of New York State Education Law Section 2-d and related Regulations of the Commissioner of Education ("Section 2-d"). To the extent that any term of the Agreement conflicts with the terms of this Exhibit, the terms of this Exhibit shall apply and be given effect.

As used in this Exhibit, the term "student data" means personally identifiable information, as defined in New York Education Law Section 2-d, from student records that Frontline receives from Customer or from a participating school district.

As used in this Exhibit, the term "teacher or principal data" means personally identifiable information from the records of an educational agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of New York Education Law Sections 3012-c and 3012-d.

As used in this Exhibit, the term "protected data" means student data and teacher or principal data

1. Frontline agrees that the security, confidentiality, and integrity of protected data shall be maintained in accordance with state and federal laws that protect the confidentiality of personally identifiable information, and also in accordance with Customer's Parents Bill of Rights for Data Security and Privacy, provided below.

2. Frontline agrees that, to the extent applicable, it will disclose protected data received from Customer or a participating school district only to those officers, employees, and agents who need access to provide the contracted services. Frontline further agrees that any of its officers or employees, and any officers or employees of any assignee or subcontractor of Frontline who have access to personally identifiable information will receive training on the federal and state law governing confidentiality of such data prior to receiving access to that data.

3. The exclusive purpose for which Frontline is being provided access to protected data is for providing Customer and its participating school districts with the functionality of the Products or Services accessed by each participating school district pursuant to a cooperative educational service agreements (CoSer) with Customer. Protected data received by Frontline, or by any assignee of Frontline, from Customer or a participating school district shall not be sold or used for marketing purposes.

4. The initial term of this Agreement expires on June 30, 2020 but the Agreement may be ~~automatically~~ extended for one or more 12-month periods. Upon expiration of this Agreement without a successor agreement in place, Customer may request that Frontline delete all protected data previously received from Customer or a participating school district that has not made alternative arrangements with Frontline to continue using Frontline Services. Frontline shall (at Customer's or the participating school district's expense) provide commercially reasonable support to Customer to extract data from Frontline Services in a format suitable for transfer to another service or platform.

5. In the event that a teacher or principal wishes to challenge the accuracy of teacher or principal data, they shall utilize the appeal process in the APPR Plan of their employing school district. In the event that a parent, student, or eligible student wishes to challenge the accuracy of student data concerning that student or eligible student, that challenge shall be processed through the procedures provided by the student's district of enrollment for amendment of education records under the Family Educational Rights and Privacy Act (FERPA).

6. Student data transferred to Frontline by Customer or a participating school district will be stored in electronic format on systems maintained by Frontline or subcontractor of Frontline in a secure data center facility, or a data facility maintained by a board of cooperative educational services, in the United States. Frontline will take measures aligned with industry best practices and the NIST Cybersecurity Framework and reasonably designed to protect the privacy and security of protected data while it is stored in such facility. Such measures include, but are not necessarily limited to disk encryption, file encryption, firewalls, and password protection.

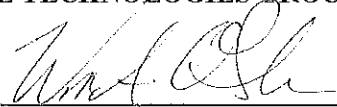
7. Frontline acknowledges that it has the following obligations with respect to any protected data received from Customer or a participating school district and any failure to fulfill one of these statutory obligations shall be a breach of the underlying Agreement:

- limit internal access to education records to those individuals that are determined to have legitimate educational reasons in compliance with Section 2-d and FERPA;
- not use education records for any purpose other than those explicitly authorized in this Agreement;
- not disclose any personally identifiable information to any other party who is not an authorized representative of Frontline, Customer, or a participating school district using the information to carry out that Party's obligations under this Agreement, unless (1) that other party has the prior written consent of the parent or eligible student, or (2) the disclosure is required by statute or court order, and notice of the disclosure is provided to the source of the information no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order;
- maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of personally identifiable information in its custody;
- use encryption technology that complies with New York Education Law Section 2-d and related Commissioner Regulations to protect data while in motion or in its custody from unauthorized disclosure;
- notify the educational agency from which student data is received of any breach of security resulting in an unauthorized release of student data by Frontline or its assignees in violation of state or federal law, or of contractual obligations relating to data privacy and security in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after discovery of the breach; and
- ensure by contractual agreements or other legally binding measures that any subcontractor, assignee, or other agent (including any Hosting Service Provider) to whom Frontline discloses protected data will comply with the same data security and privacy standards required of Frontline under this agreement and applicable state and federal laws.

Contractor's signature below shall also constitute an acknowledgement, acceptance, and signature of ESBOCES' or participating school district's Parents' Bill of Rights.

FRONTLINE TECHNOLOGIES GROUP, LLC D/B/A FRONTLINE EDUCATION

BY:



William A. O'Shea
Chief Financial Officers

DATED: May 11, 2023