SCHEDULE E

EDUCATION LAW 2-d RIDER

New York State Education Law 2-d was enacted in 2014 to address concerns relative to securing certain personally identifiable information. In order to comply with the requirements of Education Law 2-d, educational agencies and certain third-party contractors who contract with educational agencies must take certain additional steps to secure such data. These steps include enacting and complying with a Parents' "Bill of Rights" relative to protected data, ensuring that each third-party contractor has a detailed data privacy plan in place to ensure the security of such data, and that each third-party contractor sign a copy of the educational agency's Parents' Bill of Rights, thereby signifying that the third-party contractor will comply with such Parents' Bill of Rights. This Agreement is subject to the requirements of Education Law 2-d and SchoolSource Technologies, LLC (the "Contractor") is a covered third-party contractor.

In order to comply with the mandates of Education Law 2-d, and notwithstanding any provision of the Agreement between the Board of Cooperative Educational Services, First Supervisory District of Suffolk County ("ESBOCES") and Contractor, including any Agreement to Terms attached thereto, to the contrary, Contractor agrees as follows:

Contractor will treat "Protected Data" (as defined below) as confidential and shall protect the nature of the Protected Data by using the same degree of care, but not less than a reasonable degree of care, as the Contractor uses to protect its own confidential data, so as to prevent the unauthorized dissemination or publication of Protected Data to third parties. Contractor shall not disclose Protected Data other than to those of its employees or agents who have a need to know such Protected Data under this Agreement. Contractor shall not use Protected Data for any other purposes than those explicitly provided for in this Agreement. All Protected Data shall remain the property of the disclosing party. As more fully discussed below, Contractor shall have in place sufficient internal controls to ensure that ESBOCES' and/or participating school districts' Protected Data is safeguarded in accordance with all applicable laws and regulations, including, but not limited to, the Children's Internet Protection Act ("CIPA"), the Family Educational Rights and Privacy Act ("FERPA"), and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and Part 121 of the Regulations of the Commissioner of Education, as it may be amended from time-to-time if applicable.

"Protected Data" includes any information rendered confidential by State or federal law, including, but not limited to student data, student demographics, scheduling, attendance, grades, health and discipline tracking, and all other data reasonably considered to be sensitive or confidential data by ESBOCES and/or participating school districts. Protected Data also includes any information protected under Education Law 2-d including, but not limited to:

> "Personally identifiable information" from student records of ESBOCES and/or participating school districts as that term is defined in § 99.3 of FERPA,
>
> -AND-
>
> Personally identifiable information from the records of ESBOCES and/or participating school districts relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§3012-c and 3012-d.

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any Protected Data shall comply with New York State Education Law § 2-d. As applicable, Contractor agrees to comply with ESBOCES' policy(ies) on data security and privacy. Contractor shall promptly reimburse ESBOCES and/or participating school districts for the full cost of notifying a parent, eligible student, teacher, or principal of an unauthorized release of Protected Data by Contractor, its subcontractors, and/or assignees. In the event this Agreement expires, is not renewed or is terminated, Contractor shall return all of ESBOCES' and/or participating school districts' data unless otherwise provided, including any and all Protected Data, in its possession by secure transmission.

Data Security and Privacy Plan

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any of ESBOCES' and/or participating school districts' Protected Data, shall maintain a Data Security and Privacy Plan which includes the following elements:

1. Specifies the administrative, operational and technical safeguards and practices in place to protect personally identifiable information that Contractor will receive under the contract;

2. Demonstrates Contractor's compliance with the requirements of Section 121.3 of Part 121;

3. Specifies how officers or employees of the Contractor and its assignees who have access to student data, or teacher or principal data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;

4. Specifies how Contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;

5. Specifies how Contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the educational agency;

6. Specifies whether Protected Data will be returned to ESBOCES and/or participating school districts, transitioned to a successor contractor, at ESBOCES' and/or participating school districts' option and direction, deleted or destroyed by the Contractor when the contract and/or the Agreement to Terms is terminated or expires.

Pursuant to the Plan Contractor will:

1. Have adopted technologies, safeguards and practices that align with the NIST Cybersecurity Framework referred to in Part 121.5(a);

2. Comply with the data security and privacy policy of ESBOCES; Education Law § 2-d; and Part 121;

3. Have limited internal access to personally identifiable information to only those employees or subcontractors that need access to provide the contracted services;

4. Have prohibited the use of personally identifiable information for any purpose not explicitly authorized in this contract;

5. Have prohibited the disclosure of personally identifiable information to any other party without the prior written consent of the parent or eligible student:

   a. except for authorized representatives such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with state and federal law, regulations and its contract with the educational agency; or

   b. unless required by statute or court order and Contractor has provided a notice of 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 disclosure is expressly prohibited by the statute or court order.

6. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in our custody;

7. Use encryption to protect personally identifiable information in its custody while in motion or at rest; and

8. Not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

In the event Contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the third-party contractor by state and federal law and contract shall apply to the subcontractor.

Where a parent or eligible student requests a service or product from a third-party contractor and provides express consent to the use or disclosure of personally identifiable information by the third-party contractor for purposes of providing the requested product or service, such use by the third-party contractor shall not be deemed a marketing or commercial purpose prohibited by the Plan.

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

SCHOOLSOURCE TECHNOLOGIES, LLC

BY: ______________________ **DATED:** 5/25/2021

DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN IS ATTACHED HERETO AND INCORPORATED HEREIN.

DATA SECURITY AND PRIVACY PLAN

SchoolSource Technologies, LLC - Data Security and Privacy Plan

New York State Education Law 2-d was enacted in 2014 to address concerns relative to securing certain personally identifiable information. In order to comply with the requirements of Education Law 2-d, SCHOOLSOURCE TECHNOLOGIES, LLC hereby establishes the following data security and privacy plan:

SCHOOLSOURCE TECHNOLOGIES, LLC will treat "Protected Data" (as defined below) as confidential and shall protect the nature of the Protected Data by using the same degree of care, but not less than a reasonable degree of care, as it uses to protect its own confidential data, so as to prevent the unauthorized dissemination or publication of Protected Data to third parties. SCHOOLSOURCE TECHNOLOGIES, LLC shall not disclose Protected Data other than to those of its employees or agents who have a need to know such Protected Data under this Agreement. SCHOOLSOURCE TECHNOLOGIES, LLC shall not use Protected Data for any other purposes than those explicitly provided for in its agreement with the disclosing party from which it received Protected Data. All Protected Data shall remain the property of the disclosing party. As more fully discussed below, SCHOOLSOURCE TECHNOLOGIES, LLC shall have in place sufficient internal controls to ensure that Protected Data is safeguarded in accordance with all applicable laws and regulations, including, but not limited to, CIPA, FERPA and HIPAA, if applicable.

"**Protected Data**" includes any information rendered confidential by State or federal law, including, but not limited to student data, student demographics, scheduling, attendance, grades, health and discipline tracking, and all other data reasonably considered to be sensitive or confidential data by a customer. Protected Data also includes any information protected under Education Law 2-d including, but not limited to:

> "Personally identifiable information" from student records of an educational agency as that term is defined in §99.3 of the Family Educational Rights and Privacy Act (FERPA),
>
> -AND-
>
> 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 Education Law 3012-c

State, federal, and local data security and privacy contract requirements will be implemented by utilizing Best practices and industry standards with respect to data storage, privacy and protection, including, but not limited to encryption, firewalls, passwords, protection of off-site records, and limitations of access to stored data to authorized staff shall be implemented as follows:

Data

- Data is encrypted between end points from the source to the receiver.
- Databases have their own unique user and passwords in order to gain access.
- Users need a user ID and password in order to gain access to a database in addition to login credentials to gain access to a server.
- There are multiple login and password requirements before a user can access data creating a layered defense for access and data controls.
- Data is stored within a server that is cloud based and has been audited to meet SOC, COBIT, and SAS 70 requirements from internal and external auditors.
- Governance and policies for the server, security, networks, and access protocols are reviewed on a daily basis.
- All elements of the process for accessing and storing data has been audited internally following the Global Technology Audit Standards manuals that are the industry practices for technology worldwide.

Users

- Data is accessed through users that have been provided specific permissions based on the level of employee and purpose for accessing data. Protocols for requests and permissions are formal with tiered permission levels for approval.
- Data is not accessed without first submitting a password, then an authentication is sent via text to the person gaining access to data elements. If the authentication key is not returned correctly, the person will be locked out from continuing to gain access to the data.
- Once authentication is correctly entered by the user, the user will be requested to enter their unique password again prior to accessing data elements.

Hardware and Software

- All hardware that is to be included within the network mapping is tested and reviewed for weaknesses that may create intrusion points for unauthorized hackers or slippage for potential compromising network threats such as ransomware or viruses, etc.
- All software that is to be loaded onto the server is reviewed for patches that remove weaknesses for potential backdoor threats to the server.
- All PC's that are gaining access to the server are required to maintain an all inclusive virus, malware and privacy detection product.
- Hardware that is not protected will be locked out of the server and any databases housed on the server.

Measures to secure Protected Data and to limit access to such data to authorized staff will include:

Monitoring

- Alerts are used to mitigate any intrusions to the cloud servers and data. This is a monitoring of unwelcome access 24/7. The cloud is authenticated and the keys for authentication are changed continually.

- Any intruders identified through the dashboards for monitoring will shut down the IP address immediately and access will be halted. The IP address will be rendered useless and data shredded immediately.
- All access statistics and errors produced by users is logged and reviewed for escalation of issues to the point of revoking access to the server and databases.
- Mobile devices have limited access to the server and databases used. The mobile devices are used for communication access points such as emails or text messaging.
- Emailing of confidential data is prohibited if the document, spreadsheet, PDF, etc. is not sent through a controlled email server. The use of Dropbox or Adobe is used for large files with access limited in time and credentials to access the data are created.

Subcontractors, persons or entities with which SCHOOLSOURCE TECHNOLOGIES, LLC will share Protected Data, if any, will abide by the requirements of this data security and privacy plan, and any contractual obligations with respect to Protected Data set forth in the agreement with the disclosing party.

Internal access to Protected Data shall be limited to those individuals that are determined to have legitimate educational interests.

Protected Data shall not be used for any other purposes than those explicitly authorized by contract with an educational agency.

Protected Data shall not be re-disclosed to any third-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 New York State Education Department, educational agency, 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;

Reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of Protected Data shall be maintained.

Encryption technology shall be used to protect data while in motion or in SCHOOLSOURCE TECHNOLOGIES, LLC custody from unauthorized disclosure.