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 Edupoint Educational Systems, LLC ("Contractor" or "EES") 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 sub-contractors 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.

NAME OF CONTRACTOR:_____

BY: _____ **DATED:**_____

DATA PRIVACY AND SECURITY PLAN

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

Attachment 6

Client Data Protection and Security Policy

Version 2.1

Updated May 14, 2018

1. **Purpose**:

The Purpose of this policy is to improve the safeguarding of client data thereby ensuring that no Edupoint Educational Systems (EES) Staff can be implicated in an unauthorized use of partner school district student, staff, or parent data. Edupoint and each of EES Staff has a legal and moral responsibility to prevent misuse of client data that might result in physical emotional, or economic harm to any individual whose personal information is stored within District databases either created and supported by Edupoint's software products or provided for data conversion or integration purposes.

2. **Background:**

Certain EES Staff are required to work with client confidential information on a daily basis, and have a duty to protect this information from loss, theft or misuse. This responsibility exists whether the information is in paper or electronic form.

3. **Policy:**

It is the responsibility of the individual EES Staff to safeguard any and all Client Data and under no circumstances should Client Data be stored on any portable devices and/or portable media.

4. **Procedure:**

The following procedures identify specific process around the preparation, access and use of Client Data.

4.1. All EES Staff will attend and complete a *Client Data Protection and Security Orientation* where the details of handling sensitive Client Data are reviewed.

4.2. Subsequent to the completion of the *Client Data Protection and Security Orientation*, all ESS Staff will sign a *Staff Client Data Protection and Security Acknowledgement* form prior to accessing any Client Data.

4.3. All EES Staff will have an appropriate security background check performed prior to any Client Data access.

4.4. No Client Data shall be removed from any client facility, in any format, paper or electronic.

4.5. No Client Data shall be downloaded or stored on any portable computer, portable device or portable media at any time except as indicated in this policy.

4.6. At no time shall any staff be in direct possession of Client Data on any portable computer, portable device or portable media.

4.7. Customer report outputs may only be printed at an EES facility (Mesa, AZ or Irvine, CA) and must be secured at all times. Disposal is required and must be achieved via depositing in confidential shredding bins.

4.8. *Customer requests:* At times customers will request EES Staff, typically while onsite, to accept Client Data in a portable format (paper or via portable media). The following indicates the procedure for handling of these requests:

4.8.1. All customer requests for EES Staff to take physical printed reports, screen captures, etc. are required to be electronically sent via email or submitted as a support ticket.

4.8.2. All customer requests to send data must be sent via the EES secure FTP site.

4.9. The only EES product data allowed on portable equipment is EES Demonstration Data.

5. **Access to Client Data**:

Various job duties require access to customer data such as development, customer service problem troubleshooting, and data conversion. In these cases, customer data access is permitted either directly at the customer site or directly at an EES secured Facility located at 1955 S. Val Vista Dr, Suite 200, Mesa, AZ 85204.

5.1. Access at Client Site

Access to customer data existing at a customer site is permitted with Clients permission by either of the following methods:

- While physically onsite
- Remotely accessed via a secure VPN connection

In both cases client data is never stored on any portable computer, portable device or portable media.

5.2. Access at EES Secured Facility

Access to customer data within EES Secured Facility is permitted by either of the following methods:

- While physically onsite
- Remotely accessed via a secure VPN connection

In both cases client data is never stored on any portable computer, portable device or portable media outside of EES Secured Facility.

5.3 Setup of Customer Data within EES secured Facility

5.3.1 FTP

Data is allowed to be uploaded by customers to EES's FTP site and subsequently accessed in one of EES's secure facilities. Only the designated Customer Data Manager (CDM) or assigned designee will be provided access to the FTP site. Staff will wait for the CDM or assigned designee to perform the Data Cleansing Process (DCP – noted in section 6) before access to the data will be allowed.

5.3.2 Via Device

Client provides data via a device and not via FTP. EES can only accept the data via a device if the following procedures are followed:

- Client staff brings data to EES Secured Facility
- Data is immediately downloaded to EES server as if the data was uploaded via EES FTP site; Client staff must wait for the data copy to complete
- Client Staff leaves with possession of data brought to EES Secured Facility
- Data is then cleansed per the Data Cleansing Process

5.3.3 Direct Secure Download

Client provides data to EES via a direct secure download from Client's secured facility. EES can only accept the data via a secure download if the following procedures are followed:

- Approved EES staff uses EES desktop in EES Secured facility to download data
- Data is immediately downloaded to EES server as if the data was uploaded via EES FTP site
- Data is then cleansed per the Data Cleansing Process

5.3.4 QA Hosted Client Data

This section applies to client provided data that has been cleansed as outlined in the Data Cleansing Process (DCP – noted in section 6) and it is determined that Edupoint must provide access to the customer so they can assist in the resolution of an open issue.

- The Client will provide the data using one of the approved methods outline above
- HTTPS (SSL) Connections must be used to host the data in the QA Site
- All Local Synergy user passwords must be set to a complex password over 8 characters in length
- All Users must be set to Exempted from LDAP so that new local Synergy Password will be used.

5.4 Specific Client Data Access – EES Staff roles:

The following enumerates specifics of EES Staff role access to Client Data and the expected method by which the EES Staff are to accomplish required work:

i. **Implementation:**

Description: Any EES Staff tasked with performing data conversion, implementation support, training or other related tasks in support of customers during the implementation of EES products.

Method of Access: EES Staff performing any implementation task will perform all data activities directly on customer equipment. If software defects are discovered and troubleshooting needs to occur, with clients permission and oversight, the EES Staff will backup and upload Client Data to EES secure FTP site using customer FTP limited account access Id/password (which is available to all Implementation staff), and then follow typical process indicated above in section Setup of Customer Data within EES.

ii. **Customer Resource Center (CRC):**
Description: Any EES Staff tasked with directly supporting customers to resolve customer reported issues or performing account management tasks (Release Management or Systems Management).

Method of Access: EES Staff performing support tasks can access Client Data remotely via secure VPN connection into customer environments or access cleansed Client Data within EES Secured Facility (on EES servers). In no case will client data be copied to CRC staff local desktop. If uncleansed data is required for troubleshooting, the Staff shall request from their Director/VP permission to receive access to the uncleansed data. The CDM or assigned designee shall provide access to the uncleansed data upon receipt of email from the Director/VP authorizing the Staff access to the uncleansed data. The CDM or assigned designee shall restore the uncleansed data to a secure location, with restricted access. The DCP will be performed as outlined in the policy with the exception of the specific areas required for troubleshooting the particular issue from the request.

iii. **Quality Assurance (QA):**
Description: Any EES Staff tasked with testing EES product Targeted Updates, Continuous Enhancements or Releases.

Method of Access: EES Staff performing testing tasks will access cleansed Client Data within EES Secured Facility (either on EES servers on QA Staff local desktop – non-portable secured workstation). If uncleansed data is required for testing, the Staff shall request from their Director/VP permission to receive access to the uncleansed data. The CDM or assigned designee shall provide access to the uncleansed data upon receipt of email from the Director/VP authorizing the Staff access to the uncleansed data. The CDM or assigned designee shall restore the uncleansed data to a secured location, with restricted access. The DCP will be performed as outlined in the policy with the exception of the specific areas required for testing the particular issue from the request.

iv. **Development**:
Description: Any EES Staff tasked with developing new EES product features or correcting EES product defects.

Method of Access: EES Staff performing development tasks will access cleansed Client Data within EES Secured Facility (either on EES servers or on Developer Staff

local desktop - non portable secured workstation). Data access on Staff local desktop is provided since development Staff modifies the database structure during tasks that would make the database unstable in a shared environment. If uncleansed data is required for troubleshooting the staff shall request from their Director/VP permission to receive access to the uncleansed data. The CDM or assigned designee shall provide access to the uncleansed data upon receipt of email from the Director/VP authorizing the Staff access to the uncleansed data. The CDM or assigned designee shall restore the uncleansed data to a secured location, with restricted access. The DCP will be performed as outlined in the policy with the exception of the specific areas required for troubleshooting the particular issue from the request.

v. **Content Development**:
Description: Any EES Staff tasked with developing or editing EES documentation including but not limited to Edupoint Technical Notifications (ETN), Manuals, Release Notes, Quick Reference Guides (QRG), and User Guides.

Method of Access: EES Content Development staff is not permitted to expose any Client Data through documentation either printed or in electronic form. EES Content Development staff with access to the EES FTP site is only allowed access to upload files to the documentation folders. No client school district student, staff, or parent data shall be exposed in any form of documentation. All screenshots used in documentation shall be taken from EES QA Demonstration web sites. If a screenshot is required from other than a QA Demonstration web site, all client school district student, staff, or parent data shall be changed to fictitious information regarding names or any other identifiable information. At the least, identifiable information must be blurred out, using tools available with screen capture software such as Snagit and/or the Windows snipping tool.

vi. **EES Other Staff**:
Description: Any EES Staff not previously categorized above are included in this group.

Method of Access: EES Other Staff is not permitted direct access to Client Data. Any additional activities requested of EES Other Staff (e.g. demonstrations, documentation, video recordings, and regression testing in preparation of a major Release) shall be performed on EES demonstration data. If uncleansed data is required for troubleshooting, the staff shall request from the CDM or assigned designee access to the uncleansed data. The CDM or assigned designee shall restore the uncleansed data to a secure location, with restricted access. The DCP will be performed as outlined in the policy with the exception of the specific areas required for troubleshooting the particular issue from the request.

2. **Data Cleansing Process (DCP):**
The following indicates the specific steps in the process required to be performed on Client Data by CDM prior to making available to EES Staff needing access to perform work:

3. **Definitions:**

Client Data – Any information relating to any individual form any client either in electronic or physical printed form.

Client Data Orientation – EES training used to ensure all Staff understand and accept the Client Data Policy.

Customer Data Manager (CDM) – Staff identified within EES responsible for handling Client Data.

Data Cleansing Procedure (DCP) – Procedure identified used to pre-cleanse Client Data to remove sensitive person data not necessary for trouble shooting, development, and other valid work related activities.

EES – Edupoint Educational Systems.

EES Demonstration Data – Edupoint created demonstration data that has no identifiable "real" student, parent or staff information. This is the only data to be used in client facing interactions, including but not limited to screenshots, videos, PowerPoint presentations and webinars.

EES Secure Facility – Either the Mesa, Arizona office or the Irvine, California office. Both facilities are secured with recorded security cameras and key/code access for tracking all entry and exit into and out of the facilities.

EES Contractor – Any Edupoint contractor or agent.

ETN – Edupoint Technical Notification.

Portable Devices – Tools such as laptops, external hard drives, cell phones (including Android, and iPhone devices), Tablet PCs, other USB memory devices and cameras (digital, non-digital, and video).

Portable Media – Any tool used to store and/or transport information any distance such as floppy disks, CDs, DVDs, USB memory sticks, flash drives, or smart cards.

QRG – Quick Reference Guide.

Staff Client Data Protection and Security Acknowledgement

Portable and remote Computing

All mobile computing (i.e. laptops, tablets, cell phones, USB flash drives, and handheld devices) should be properly physically secured, locked to prevent devices from theft, and must be password protected using strong authentication methods.

Passwords Protecting Workstations and Other Computing Devices
EES Staff are responsible for helping maintain the security of workstations and other computing devices by striving to protect them from unauthorized access and malicious software infections (e.g. viruses, worms, and spyware). All PCs, laptops, cell phones, and computer workstations should be secured with a password-protected screensaver with the automatic activation feature set to 30 minutes to prevent unauthorized access to the device.

Security
Passwords should be a minimum of 6 characters with a combination of letters and numbers. Staff are responsible for protecting their passwords. Passwords are not to be shared, copied, overheard, requested, or disclosed. Staff should take precautions and practice secure password management. Staff should not tamper with the baseline security configuration on their workstations. Staff shall consult the Information Technology department (480.633.7500.7575) for guidance on protecting their computing devices.

Protect Passwords, Identification Cards, and Other Access Devices
Passwords, identification cards, and other access devices are used to authenticate the identity of individuals and gain access to Edupoint resources. Each staff is responsible for protecting the access devices assigned to her or him and shall not share the devices with others. If an access device is compromised, lost or stolen, the staff shall report this to the Information Technology department (480.633.7500.7575) as soon as possible so that the access device is not used by an unauthorized person.

Protect against Physical Access by Unauthorized Personnel
Desktop computers should be locked while unattended in order to reduce the occurrence of unauthorized access. Password-protected screensaver must be set with the automatic activation feature set to 30 minutes to prevent unauthorized access to the device.

Report Security Violations, Malfunctions, and Weaknesses
Staff shall report security related events; known or suspected violations of *Staff Client Data Protection and Security Acknowledgement*; and inappropriate, unethical and illegal activities involving Edupoint resources. Users shall call the Information Technology department (480.633.7500.7575) for incident reporting.

User Acknowledgement Agreement
I acknowledge that I received and read the *Staff Client Data Protection and Security Acknowledgement* and the *Client Data Protection and Security Policy*. I understand that I must comply with these standards when accessing and using Edupoint resources and interacting with Client Data. I acknowledge that Edupoint will be monitoring the network to ensure that I am complying with Edupoint policies. If I fail to comply with the Edupoint policies or violate the Edupoint policies, Edupoint reserves the right to terminate my employment and possibly seek legal actions.

Signature:_____ Date:_____

Print Name:_____

Edupoint's Student Data Privacy Policy

EDUPOINT complies at all times with the requirements of the Family Educational Records Privacy Act ("FERPA") regarding the confidentiality and handling of student records and information, including but not limited to student names, parent names, addresses, grades, disciplinary actions, attendance, health, and other personal matters particular to the respective students as supplied by the school district. EDUPOINT only accesses student information pursuant to prior written parental consent, legitimate educational interests in performing duties on behalf of the District or other provisions of federal and state law permitting access to confidential student information.

EDUPOINT understands and agrees to the following responsibilities regarding maintaining the security and confidentiality of District's student data:

- EDUPOINT acknowledges that the data that will be entered into the Licensed Software Products includes personally identifiable student information that is confidential and proprietary to the respective school districts, and subject to State and Federal confidentiality laws and regulations including but not limited to FERPA.
- EDUPOINT takes all reasonable measures to ensure that the Licensed Software Products are equipped with current industry-standard security safeguards, including but not limited to encryption, with the intent to prevent unauthorized access to, use, or disclosure of, the confidential data and information that will be entered into the Licensed Software Products.
- EDUPOINT instructs all of EDUPOINT's staff who require access to confidential information in order to carry out their professional responsibilities about the requirements for handling confidential information, and requires each person who will have access to confidential information to sign an agreement to comply with EDUPOINT confidentiality provisions.
- EDUPOINT uses all available and commercially reasonable methods to design and code the Licensed Software Products to function in such a manner that does not permit access to personally identifiable student information by individuals other than authorized representatives of an appropriate school district and/or EDUPOINT who have legitimate educational interests in the information, specifically, those who require access to the data stored and analyzed on the Licensed Software Products in order to be able to carry out their professional responsibilities. Access to personally identifiable student information by parents and students for purposes of review and correction is determined by the rules of client school districts.
- EDUPOINT will not contact any individuals included in the data sets without obtaining advance written authorization from the applicable school district, or as authorized, permitted and/or required under applicable law, rule or regulation.
- EDUPOINT shall not disclose any school district confidential student data, with or without personally identifying information, to any other individuals, agencies, or organizations (except disclosures to local, State or Federal agencies as may be required under applicable law), without first obtaining, in cooperation with the applicable school district, prior written consent of the parent or eligible student.
- EDUPOINT shall not use a school district's confidential student data, with or without personally identifying information, in any form, or in any way, for any purpose other than the respective school district's purposes (except disclosures to local, State or Federal agencies as may be required under applicable law).

- To the extent applicable, EDUPOINT shall keep all confidential student data furnished by a school district in a space as may be commercially reasonable to physically and electronically keep such information secure from unauthorized access. Confidential student data shall be stored and processed in a way commercially reasonably calculated so that unauthorized persons cannot retrieve nor alter the information by means of a computer, remote terminal, or other means. No confidential student data will be stored, except on a temporary basis, on laptop computers or other portable computing devices or media, e.g., flash drives, etc. Confidential student data will be promptly deleted from any such device as soon as it is no longer needed for immediate operational purposes. Such devices will be reasonably secured during such time as confidential student data is stored on them. Other than as maintained and used on a particular school district's devices and equipment, confidential student data will only be used on EDUPOINT devices and equipment.
- EDUPOINT agrees that a school district's confidential data shall be returned and/or destroyed when no longer needed for district authorized purposes upon written authorization from the applicable school district. All destruction of a school district's confidential data shall be accomplished by utilizing an approved method of confidential destruction, including shredding, burning or certified/witnessed destruction for physical materials and verified erasure of magnetic media using approved methods of electronic file destruction.
- Notwithstanding anything contained herein to the contrary, EDUPOINT and its officers, managers, employees, agents and contractors shall have the right to disclose any confidential data or information in the event EDUPOINT or any such officers, managers, employees, agents and contractors, are compelled to do so by order of any State or federal court. If EDUPOINT receives a request for a school district's confidential student data, or if such records are compelled by order of any state or federal court or other governmental authority, EDUPOINT will provide the particular school district with written notice of the request or order.
- Further, notwithstanding anything to the contrary in this policy statement, Edupoint does not, and will not, sell any confidential student data at any time, for any reason. Any company with whom Edupoint may merge or to which it may sell its student data software business in the future, shall be encouraged to abide by the terms of the above policy. In addition, clients would reserve the right to refuse to send future data, and can have existing data returned to them, if above policy is not honored.
- Material changes to this policy will be accompanied by email notification to clients and a request that clients respond with questions or concerns.