Attachment C

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 EMS LINQ, 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 personally identifiable: student data, student demographics, scheduling, attendance, grades, health and discipline tracking. Protected Data also includes all other data reasonably considered to be sensitive or confidential data by ESBOCES and/or participating school districts that ESBOCES and/or the participating school district has identified to Contractor in writing as sensitive or confidential data of ESBOCES and/or the participating school district. 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, to the extent ES BOCES policies reflect the applicable law, Contractor agrees to comply with ESBOCES' policy(ies) on data security and privacy provided to Contractor in advance of executing this Agreement. To the extent attributable to the LINQ's employees, agents, or personnel actions and/or omissions, Contractor shall promptly reimburse ESBOCES and/or participating school districts for the 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 delete all of ESBOCES' and/or participating school districts' Protected Data, in its possession by secure transmission.

*Modified to reflect LINQ's clarifications

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, or 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, ESBOCES or the 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.

<CONTRACTOR>

BY: _____ **DATED:** 4/17/25

DATA PRIVACY AND SECURITY PLAN

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

Please see LINQ's responses on the following pages.

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;

   In compliance with the contractual requirement to protect personally identifiable information (PII) under the NIST Cybersecurity Framework, FERPA, and the New York Parents' Bill of Rights, the Contractor represents and warrants that it has implemented the following safeguards and practices:

   1. Data Encryption: PII is encrypted both in transit and at rest using industry-standard encryption protocols (such as TLS and AES-256) to ensure confidentiality and data protection.
   2. Access Controls: Strict role-based access controls (RBAC) are enforced to limit access to PII to authorized personnel only, ensuring that access is based on the principle of least privilege.
   3. Monitoring and Incident Detection: Continuous monitoring and advanced intrusion detection systems (IDS) are in place to identify and alert on potential unauthorized access or anomalies involving PII.
   4. Data Breach Notification: A formal incident response plan is established to address potential data breaches, which includes prompt notification to affected parties in compliance with FERPA and New York State requirements.
   5. Training and Awareness: All employees and contractors undergo regular training on data privacy and security best practices, with specific focus on compliance with FERPA and the protection of student data.
   6. Third-Party Vendor Compliance: Any subcontractors or third-party services used by the Contractor are subject to the same stringent data protection requirements, and agreements are in place to ensure compliance with applicable laws and regulations.
   7. Data Minimization and Retention: PII collected and retained is limited to the minimum necessary for the purposes of the Agreement, and all data is securely disposed of once it is no longer required.
   8. Risk Management: Regular risk assessments are conducted to evaluate and address potential vulnerabilities in the handling of PII, in alignment with the NIST Cybersecurity Framework's Identify and Protect functions.

   The Contractor ensures that these safeguards are in full effect to protect the integrity, confidentiality, and availability of PII, in accordance with applicable federal and state laws.

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

   EMS LINQ, LLC cares about your privacy, and we are committed to responsibly handling your personal information. Our Privacy Policy explains how LINQ collects, uses, discloses, and protects personal information that we collect from and about you through our Websites and Solutions. LINQ has thoroughly vetted our online privacy agreement and procedures for managing student data. This includes assertions to never use student data for marketing purposes, to define provisions for the duration and retention of data, and how LINQ reconciles inquiries or requests

to remove personal information from our systems among others. Our policy is located here: https://www.linq.com/privacy-policy/

More importantly, LINQ embraces data security at its core. This includes encrypting all data at rest and in transit, utilizing multiple levels of data security, both physical and logical, and educating our employees on the importance of data security. Additionally, LINQ enables Purchasing Schools/BOCES to configure strong security controls to ensure additive security provisions. Lastly, LINQ has full audit history and traceability of all transactions allowing administrators to interrogate and understand who accesses our platform, what transactions they are performing, and to take any action on actions that may compromise student data security.

LINQ further publishes its Security Statement here: https://www.linq.com/legal/security-statement/

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;

The Contractor acknowledges that federal and state laws protect the confidentiality of personally identifiable information (PII) of students, as well as, to some degree, the PII of teachers and principals from the Purchasing Schools/BOCES. To comply with these laws and ensure that all officers, employees, subcontractors, or agents who will have access to this data are appropriately trained, the Contractor represents and warrants the following:

1. Comprehensive Training Program: Prior to accessing the personally identifiable information of students, teachers, or principals, all relevant personnel will receive comprehensive security awareness and data privacy training through the LINQ LMS system.
2. Security Awareness Training: Personnel will complete security awareness training, which covers key topics such as data protection, security best practices, and handling sensitive information, ensuring they are fully aware of their responsibilities under applicable federal and state laws.
3. Targeted Data Privacy and FERPA-Specific Training: In addition to the general security training, staff will undergo targeted data privacy training, specifically focused on the protection of PII in compliance with FERPA (Family Educational Rights and Privacy Act) and other state confidentiality laws. This training includes scenarios and guidance on proper data handling, sharing limitations, and breach response procedures to ensure they understand the legal requirements governing the confidentiality of student, teacher, and principal data.
4. Ongoing Training and Awareness: The training is not a one-time requirement. In addition to annual and periodic training, LINQ provides regular communication via email covering topics such as emerging threats and evolving scams. Additionally, LINQ periodically tests staff via simulated phishing emails.
5. Tracking and Reporting: The LINQ LMS enables us to track and verify completion of all assigned training modules.

By leveraging the comprehensive resources of LINQ LMS and incorporating specific training modules focused on FERPA and data privacy, the Contractor ensures full compliance with federal and state confidentiality laws, protecting the personally identifiable information of students, teachers, and principals of the Purchasing Schools/BOCES.

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

   The Contractor ensures that all subcontractors are held to the same data protection standards as LINQ employees. Subcontractors must:

   1. Complete data security and privacy training, including FERPA.
   2. Undergo vendor risk assessments by LINQ's Information Security Department.
   3. Adhere to contractual obligations for data security, encryption, and breach reporting.
   4. Undergo continuous monitoring and audits to ensure compliance.
   5. Follow Incident Response Protocols for any data breaches.

   These measures ensure that subcontractors comply with all federal, state, and local data protection requirements.

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;**

   The Contractor takes data privacy and security incidents seriously and has implemented the following measures to manage incidents involving personally identifiable information (PII):

   1. Monitoring and Detection: We employ continuous monitoring systems to detect anomalies, unauthorized access, or any suspicious activity. Regular security audits and vulnerability scans are conducted to proactively identify potential risks.
   2. Incident Response Plan (IRP): Our comprehensive Incident Response Plan outlines the steps to be taken immediately upon identifying a data breach or unauthorized disclosure. This includes containment, investigation, and mitigation of the breach, ensuring minimal impact.
   3. Breach Identification and Investigation: Upon detection of any suspicious activity, our security team promptly investigates the scope and cause of the incident.
   4. Notification: If a breach involving PII is confirmed, we follow legal and contractual requirements for notifying affected parties, relevant authorities, and the Purchasing Schools/BOCES within the required timeframe. We provide details about the nature of the breach, the data affected, and the steps taken to address it.
   5. Remediation: After a breach, we implement remediation steps to prevent recurrence, including patching vulnerabilities, strengthening security controls, and conducting post-incident reviews to improve our response capabilities.

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, or direction, deleted or destroyed by the Contractor when the contract and/or the Agreement to Terms is terminated or expires.**

   As part of LINQ's internal Information Security Policy and Procedures Manual, there exists an Encryption Policy that corresponds to LINQ's Data Classification Policy. The encryption policy stipulates what data should be encrypted, the approved methods, and means by which data in control of LINQ should be encrypted, including data at rest and data in transit.

End of Contract Term and Return of Data

At LINQ, we understand that as a cloud service provider, our customers are entrusting their data for the term of their subscription with us. While we hope to never lose a customer, we realize that invariably some customers, whether it is budget, technical fit, or simply a mutual parting of ways, will choose to discontinue their LINQ Nutrition service. Moreover, some vendors make it extremely difficult to off-board from their solution, choosing to believe that adding impediments will ensure long-term customer retention and, conversely, not impact overall customer satisfaction. They also lose sight of the fact that a customer's choosing to use their service does not confer any rights of ownership of data – it is your citizen's data.

We take a fundamentally different approach. We want the decision to leave LINQ to be difficult, simply because we continue to provide an exceptional product delivered by approachable staff, but not because it is technically complicated. Consequently, we provide a variety of ways to offload data, as well as provide beneficial contract provisions to facilitate an amicable departure.

Technology for Data Return

First, LINQ Nutrition makes data easily exportable through reports and APIs. Virtually any data within LINQ Nutrition can be exported. For integration with other internal systems, we utilize API, SQL, or Flat File. We support Active Directory and LDAP for user pass through. We maintain all roles and rights to information in LINQ Nutrition via our security roles.

Data Reports can be created and exported using SFA assigned FTP site or a LINQ Nutrition provided secure FTP site dedicated to the district. Reports can be sent in many formats, including Excel, PDF, HTML, and CSV. These can then be picked up on the FTP site to be ingested into any system you would like, such as SIS or accounting systems. This includes the offboarding of data from our service. API extraction is facilitated through OData (Open Data Protocol). OData is an OASIS standard that allows you to create an ODBC connection to LINQ Nutrition and have specific read-only views to extract data as needed.

Favorable Contract Terms

Second, LINQ Nutrition provides favorable contract provisions on cancellation that are unmatched in the industry. This includes a 90-day post-term window in which a limited number of users are extended read-only access and viewing to offload critical data. LINQ Nutrition does not charge for this extension beyond the renewal date. It allows for the Purchasing Schools/BOCES to offload information in a controlled manner, as well as triple check that all relevant data has been extracted. Following the 90 days and consistent with our data retention policy and MSA, LINQ Nutrition deletes customer data to ensure that PII data is not retained, avoiding the possibility of data theft because of information kept on servers long after service cancellation.

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);

In alignment with state, federal, and local data security and privacy requirements, and to remain consistent with the data security and privacy policies of Eastern Suffolk BOCES, the Contractor

will implement the following comprehensive safeguards and strategies over the term of the Agreement:

1. Compliance: Adhere to all relevant data protection laws, including FERPA, the NIST Cybersecurity Framework, Education Law 2-D (New York State), and the New York Parent's Bill of Rights.
2. Data Security and Privacy Controls: Implement robust data security measures, such as encryption (e.g., AES-256 and TLS 1.2 or higher) and access control mechanisms, including role-based access controls (RBAC) and multi-factor authentication (MFA) for systems containing sensitive data.
3. Risk Assessments and Audits: Conduct regular risk assessments and audits to evaluate and mitigate vulnerabilities in data handling and protection processes.
4. Incident Response and Breach Notification: Maintain a detailed Incident Response Plan (IRP) that includes procedures for breach notification, ensuring prompt and compliant communication with stakeholders.
5. Employee Training: Provide comprehensive data privacy and security training for all employees, with an emphasis on FERPA and other relevant regulations, to ensure awareness of their responsibilities regarding data protection.
6. Data Minimization, Retention, and Disposal: Establish and enforce a data minimization, retention, and secure disposal policy to limit PII collection to only what is necessary and ensure timely and secure deletion of data.
7. Third-Party Oversight: Ensure that all third-party vendors and subcontractors comply with applicable data protection laws and agreements through continuous oversight and contractual enforcement.
8. Policy Review and Updates: Regularly review and update data protection policies to reflect changes in state, federal, and local regulations, as well as emerging cybersecurity best practices.

By implementing these measures, the Contractor ensures the protection of personally identifiable information (PII) in full compliance with state, federal, and local requirements, as well as the data security and privacy policies of ESBOCES.

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

LINQ confirms we comply with the Education Law and are able to adhere to all ESBOCES policies that are reasonable and align with industry best practices.

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

LINQ has implemented policies, procedures, and technical controls to ensure that access to Customer Data is managed on a "need to know basis," that LINQ personnel appropriately protect their access, and that information is accessed securely.

LINQ assigns user access privileges based on the principle of least privilege, according to a user's role and business need. Documented request and approval processes must be followed to gain access to assets that are not within a user's assigned to a role. Additional controls are assigned for privileged access rights, such as administrators of applications. LINQ conducts quarterly manual reviews of user accounts and security groups to ensure access privileges remain

correctly assigned.

LINQ personnel are assigned unique user IDs which must be used to access information assets, and LINQ has implemented a password policy to ensure employees set strong passwords and protect them appropriately. Rules for sharing and inputting passwords are enforced to avoid unauthorized use and disclosure.

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

LINQ ensures personal information is limited to the purposes in our privacy policy through data minimization, strict access controls, regular audits, and clear consent processes, all enforced by internal policies and training.

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, ESBOCES or the 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.

LINQ prohibits the disclosure of PII except for authorized representatives and unless required by statue 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;

LINQ takes security very seriously. All communication and data transfers within LINQ solutions are encrypted by 256bit AES encryption. Platform administration is secured using two-factor authentication. Security is a multidimensional issue that includes both physical data center security, and application and database integrity. Data vulnerability and security issues can arise from unauthorized individuals gaining access to physical media, penetrating application data through social engineering, or simply leaving a system logged in and unattended. LINQ solutions have multiple layers of security controls designed to counteract these vulnerabilities and is described further below.

Physical Security

All LINQ datacenters are secured according to industry best practices. LINQ utilizes leading data center service providers who provide data center physical security based on a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, and biometrics. Data centers are further monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. As a person gets closer to the data center floor, security measures also increase. Access to the data center floor is only possible via a

security corridor which implements multifactor access control using security badges and biometrics. Only approved employees with specific roles may enter at any time.

Hardware and Software Security

LINQ data centers house purpose-built servers and network equipment supplied by industry leading service providers. Unlike commercially available hardware, LINQ's servers don't include unnecessary components such as video cards, chipsets, or peripheral connectors, which can introduce vulnerabilities. Production servers run a custom-designed operating system (OS) based on a stripped-down and hardened version of Windows OS. This homogeneous environment is maintained by proprietary software that continually monitors systems for binary modifications. If a modification is found that differs from the standard LINQ image, the system is automatically returned to its official state.

Network Security

From a network security perspective, only authorized services and protocols that meet security requirements can traverse the network; anything else is automatically dropped. Industry-standard firewalls and access control lists (ACLs) are used to enforce network segregation. We pass all public traffic through a Web Application Firewall.

LINQ Application Security

LINQ employs rigorous safeguards to ensure that its application and data are secure. To begin with, all LINQ data is encrypted both at rest (256-bit Advanced Encryption Standard) and in-transit. Additionally, LINQ conducts security and vulnerability scans of our application on an ongoing cadence. This includes scanning for items, including but not limited to cross-site-scripting (XSS), injection, mixed content (HTTP in HTTPS), and outdated/insecure libraries.

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

   All data is encrypted in the entire system. 256 bit AES encryption at motion and at rest.

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.

   EMS LINQ, LLC cares about your privacy, and we are committed to responsibly handling your personal information. Our Privacy Policy explains how LINQ collects, uses, discloses, and protects personal information that we collect from and about you through our Websites and Solutions. LINQ has thoroughly vetted our online privacy agreement and procedures for managing student data. This includes assertions to never use student data for marketing purposes, to define provisions for the duration and retention of data, and how LINQ reconciles inquiries or requests to remove personal information from our systems among others. Our policy is located here: https://www.linq.com/privacy-policy/

EASTERN SUFFOLK BOCES
PARENTS' BILL OF RIGHTS
FOR DATA SECURITY AND PRIVACY

Eastern Suffolk BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, parents, legal guardians and persons in parental relation to a student are entitled to certain rights with regard to their child's personally identifiable information. The Agency wishes to inform the school community of the following rights:

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 maintained by Eastern Suffolk BOCES.

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 the State is available for public review at: http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx, Or, by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to:

Claudy Damus-Makelele
Associate Superintendent for Educational Services
Eastern Suffolk BOCES
201 Sunrise Highway
Patchogue, NY 11772
cdamus@esboces.org

Or in writing to:

Chief Privacy Officer
New York State Education Department
89 Washington Avenue
Albany, New York 12234.
CPO@mail.nysed.gov

Supplemental Information Regarding Third-Party Contractors:

In the course of complying with its obligations under the law and providing educational services, Eastern Suffolk BOCES has entered into agreements with certain third-party contractors. Pursuant to such agreements, third-party contractors may have access to "student data" and/or "teacher or principal data." Each contract the Agency enters into with a third party contractor where the third party contractor receives student data or teacher or principal data will include information addressing the following:

See attached two pages for answers to these questions -

1. The exclusive purposes for which the student data or teacher or principal data will be used;

   Answer: *The successful vendor needs to confirm that any and all data (including student, teacher, and principal data) is not to be used for any purpose, other than the encryption of that data.*

2. How the third party contractor will ensure that the subcontractors, persons or entities that the third party contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements;

   Answer: *The successful vendor will be required in the bid process to describe how they will abide by data protection and security requirements.*

3. When the agreement expires and what happens to the student data or teacher or principal data upon expiration of the agreement;

   Answer: *The successful vendor will be required in the bid process to describe how they will abide by data protection and security requirements at the expiration of the agreement.*

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; and

   Answer: *Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to*:

   Claudy Damus-Makelele, Associate Superintendent for Educational ServicesEastern Suffolk BOCES, 201 Sunrise Highway, Patchogue, NY 11772
   cdamus@esboces.org;

   Or in writing to:

   Chief Privacy Officer, New York State Education Department, 89 Washington Avenue
   Albany, NY 12234
   CPO@mail.nysed.gov

5. 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, including whether such data will be encrypted.

   Answer: *The successful vendor will be required in the bid process to describe how they will ensure data is encrypted and protected.*

Third Party Contractors are required to:

1. Provide training on federal and state law governing confidentiality to any officers, employees, or assignees who have access to student data or teacher or principal data;
2. Limit internal access to education records to those individuals who have a legitimate educational interest in such records.
3. Not use educational records for any other purpose than those explicitly authorized in the contract;
4. Not disclose 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 third-party contractor provides a notice of the disclosure to the New York State Education Department, 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;

5. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable student information in its custody;
6. Use encryption technology to protect data while in motion or in its custody from unauthorized disclosure as specified in Education Law §2-d;
7. Notify Eastern Suffolk BOCES of any breach of security resulting in an unauthorized release of student data or teacher or principal data, in the most expedient way possible and without unreasonable delay;
8. Provide a data security and privacy plan outlining how all state, federal and local data security and privacy contract requirements will be implemented over the life of the contract;
9. Provide a signed copy of this Bill of Rights to Eastern Suffolk BOCES thereby acknowledging that they are aware of and agree to abide by this Bill of Rights.

This Bill of Rights is subject to change based on regulations of the Commissioner of Education and the New York State Education Department's Chief Privacy Officer, as well as emerging guidance documents.

A copy of this ESBOCES Parents' Bill of Rights must be made a part of Contractor's Data Security and Privacy Plan.

Vendor Name: EMS LINQ, LLC

The following has been pulled from the Parents' Bill of Rights section in the Education Law 2-d Rider packet. Please review and answer questions 1, 2, 3 and 5.

Supplemental Information Regarding Third-Party Contractors

In the course of complying with its obligations under the law and providing educational services, Eastern Suffolk BOCES has entered into contracts with certain third-party contractors. Pursuant to such contracts, third-party contractors may have access to "student data" and/or "teacher or principal data." Each contract Eastern Suffolk BOCES enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data will include information addressing the following:

1. The exclusive purposes for which the student data or teacher or principal data will be used;

   Answer: The student, teacher, and principal data will be utilized solely for the operation of the software or service provided under the agreement, ensuring compliance with legal requirements and data protection standards, and will not be used for any commercial purposes.

2. How the third-party contractor will ensure that the subcontractors, persons, or entities with whom the third-party contractor will share the student data or teacher or principal data, if any, will abide by data protection and security requirements;

   Answer: The third-party contractor will ensure that any subcontractors, persons, or entities with whom they share student, teacher, or principal data, if any, will abide by data protection and security requirements through strict contractual obligations, regular training, and continuous monitoring. This ensures compliance with all relevant laws and standards.

3. When the contract expires and what happens to the student data or teacher or principal data upon expiration of the agreement;

   Answer: Upon contract expiration, the customer will have a 30 to 90-day period to download or request a copy of the student, teacher, and principal data before it is securely deleted.

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 collected;

   Answer: Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to:

   Claudy Damus-Makelele, Associate Superintendent for Educational Services Eastern Suffolk BOCES, 201 Sunrise Highway, Patchogue, NY 11772 cdamus@esboces.org ;

   Or in writing to:

   Chief Privacy Officer, New York State Education Department, 89 Washington Avenue Albany,

NY 12234 CPO@mail.nysed.gov

5. 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 that such data will be protected, including whether such data will be encrypted.

   Answer: The student, teacher, and principal data will be securely stored in AWS, ensuring compliance with all relevant data protection and security requirements. LINQ employs state-of-the-art security intrusion detection and prevention services to safeguard the data. Additionally, LINQ conducts an annual SOC 2 Type II audit assessment to uphold the highest standards of data security and privacy.