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 **Bold Systems, 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, Contractor agrees to comply with ESBOCES' policy(ies) on data security and privacy provided to Contractor in advance of executing this Agreement. 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 delete all of ESBOCES' and/or participating school districts' 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, 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:** 7/1/2025

DATA PRIVACY AND SECURITY PLAN

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

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:

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.

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;

   Bold Systems does not collect student, teacher, or principal data in the ordinary course of providing services. If such data were ever furnished to us by a school district, it would be used solely to fulfill the contractual purpose and would be handled in accordance with our Data Privacy and Security Plan, which complies with Education Law §2-d.

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;

   Bold Systems does not share protected data with subcontractors. If data were ever furnished and subcontractor involvement were authorized by the educational agency, we would require signed agreements ensuring:

   - *Full adherence to Education Law §2-d*
   - *Use of data only for approved purposes*
   - *Encryption of data in transit and at rest*
   - *Secure deletion upon contract end*

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

   Bold Systems does not retain student or staff data. If any such data were provided, it would be securely deleted upon contract expiration or request. We will provide written certification of data destruction upon request.

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;

   Complaints should be directed to: the Associate Superintendent for Curriculum for your district; Or in writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 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.

If student or staff data were ever provided, it would be stored in secure U.S.-based environments protected by:

- TLS 1.2+ encryption in transit
- Role-based access control
- Regular vulnerability scanning and annual staff training

All safeguards align with the NIST Cybersecurity Framework and Education Law §2-d requirements.

7/29/25 Update -
Vendor provided their Data Privacy and Secuirty Plan - See the following two pages (11 and 12)

Bold Systems, LLC
2805 Veterans Memorial Highway, Suite 23
Ronkonkoma, NY 11779
631-676-7107

RFP # 26S-21-0710R-: Election Management Software & Services
Bid Opening: June 26, 2025

Re: Personally Identifiable Information as this term is defined pursuant to New York State Education Law Section 2-d.

STATEMENT IN LIEU OF DATA SECURITY AND PRIVACY PLAN

Bold Systems, LLC acknowledges that in the event that it receives and/or is provided with personally identifiable information, it shall, in all respects, institute and have in place sufficient protections and internal controls to ensure that personally identifiable information is safeguarded in full compliance with its obligations pursuant to New York State Education Law Section 2-d.

Vendor:	Bold Systems, LLC
Address:	2805 Veterans Memorial Highway, Suite 23 Ronkonkoma, NY 11779
Telephone Number:	631-676-7107
Authorized Signature:	Brian J. Jusas, Managing Member
Date:	7/1/2025

Bold Systems, LLC

Data Privacy and Security Plan Pursuant to New York Education Law §2-d

1. Introduction and Scope

Bold Systems, LLC ("Bold Systems") does not collect student data or teacher/principal data in the ordinary course of providing services. However, if such data were ever furnished to us by an educational agency, this Data Privacy and Security Plan ("Plan") outlines the strict protocols we would follow to protect that data in accordance with New York Education Law §2-d, 8 NYCRR Part 121, and Eastern Suffolk BOCES requirements. All Protected Data shall remain the property of the disclosing agency.

2. Compliance with Education Law §2-d

In the event Protected Data is provided, Bold Systems will:
- Comply with FERPA, COPPA, CIPA, HIPAA, Education Law §2-d, and all applicable state and federal laws and regulations
- Not sell, reuse, or disclose Protected Data for marketing or commercial purposes
- Not disclose Protected Data without prior written authorization from the educational agency or unless required by law with proper notification
- Limit internal access to only those employees with a legitimate educational interest in fulfilling the contracted service
- Retain Protected Data only as long as necessary for contract fulfillment and delete or return it thereafter as directed

3. Data Collected and Purpose

Bold Systems does not proactively collect student or staff data. If such data is provided by an educational agency, it will be used solely for the purposes outlined in the contract and not for any other purpose.

4. Data Protection Measures

If Protected Data is received, Bold Systems applies administrative, technical, and physical safeguards that include:
- TLS 1.2+ encryption for data in transit
- Role-based access control
- Staff training on privacy and data security
- Regular vulnerability scanning and compliance auditing

These practices align with the NIST Cybersecurity Framework and Part 121.5(a).

5. Third-Party Subcontractors

Bold Systems does not use subcontractors for data processing unless explicitly authorized. If subcontractor use is required, we ensure:
- Signed agreements binding them to Education Law §2-d requirements
- Use of data only for contract-necessary services
- Equivalent data safeguards
- Return or certified secure destruction of data upon termination

6. Parent Bill of Rights

Bold Systems will:
- Provide a signed copy of the ESBOCES Parents' Bill of Rights with each contract
- Honor parent rights to inspect their child's data upon request
- Direct complaints to the appropriate ESBOCES contact or NYSED Chief Privacy Officer at CPO@mail.nysed.gov

7. Data Retention and Destruction

All Protected Data provided will be deleted or securely returned within 60 days of contract expiration, or as otherwise directed. Destruction will be documented in writing.

8. Breach Notification Protocol

In the event of a breach, Bold Systems will:
- Notify the educational agency without unreasonable delay
- Include all breach details, mitigation steps, and corrective actions in the report
- Cooperate fully with ESBOCES in breach response and notifications to affected individuals

9. Training and Oversight

All staff with access to Protected Data:
- Sign confidentiality agreements
- Are subject to ongoing oversight and disciplinary enforcement

10. Data Inventory and Security Practices

Bold Systems maintains an internal data inventory, tracking:
- Types and purpose of data received
- Storage and access controls
- Audit logs and transmission protocols

Periodic reviews and compliance checks are conducted to ensure security.

11. Amendments and Updates

This Plan is reviewed annually or more frequently to comply with evolving guidance from NYSED, Commissioner regulations, and emerging best practices. Bold Systems maintains full readiness to comply with Education Law §2-d whether or not Protected Data is actively collected.