EDUCATION LAW 2-d AGREEMENT

This Education Law 2-d Agreement ("Agreement") is effective as of the date of last signature below and is by and between the **Board of Cooperative Educational Services, First Supervisory District of Suffolk County** ("**ESBOCES**" or "**Eastern Suffolk BOCES**") whose principal place of business is 201 Sunrise Highway, Patchogue, NY 11772 and **Diligent Corporation** (hereinafter "**Contractor**"), a Delaware corporation, whose principal place of business is 111 West 33rd St, 16th Floor, New York, NY 10120 ("the Agreement"). Each of ESBOCES and Contractor are a "**Party**" and are together the "**Parties.**

WHEREAS, Contractor has contracted with New York State School Boards Association ("NYSSBA") via separate agreement to resell Contractor's BoardDocs™ software-as-a-service offering (the "Service") to Boards of Cooperative Educational Services within New York State;

WHEREAS, ESBOCES has contracted with NYSSBA via separate agreement to purchase BoardDocs on behalf of its affiliated school districts;

WHEREAS, Contractor may receive or have access to student data or teacher or principal data in providing BoardDocs to participating school districts of ESBOCES, and in receiving or accessing such data Contractor is a third-party contractor under New York State Education Law 2-d;

NOW, THEREFORE, the Parties agree as follows:

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 the Contractor is a covered third-party contractor.

In order to comply with the mandates of Education Law 2-d, 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. 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 reasonable internal controls designed 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 that is uploaded to BoardDocs. Protected Data also includes any information protected under Education Law 2-d that is uploaded to BoardDocs, 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.

To the extent applicable, 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 the data security and privacy plan set forth herein. To the extent required under New York State Education Law § 2-d, subsection 6(c) and 8 NYCRR 121.10, Contractor shall promptly reimburse ESBOCES 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 by secure transmission or destroy any and all Protected Data.

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. To the extent applicable, 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 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. To the extent applicable, comply with 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.

The Parties enter into this Agreement for the limited purpose of ensuring each Party's compliance with the requirements of New York State Education Law 2-d, to the extent applicable to ESBOCES' purchase of a subscription to the Service from NYSSBA on behalf of its affiliated school districts. Contractor's obligations under this Agreement are contingent upon ESBOCES' purchase of a subscription to the Service from NYSSBA for use by its participating school districts. In the event ESBOCES no longer purchases a subscription to the Services from NYSSBA, Contractor shall have no obligations hereunder other than the obligation to return by secure transmission or destroy any and all Protected Data.

DILIGENT CORPORATION

DocuSigned by:
2DC657616BD64E7...

BY: _____ **DATED:** March 8, 2022 | 3:18 PM EST

BOARD OF COOPERATIVE EDUCATIONAL SERVICES, FIRST SUPERVISORY DISTRICT OF SUFFOLK COUNTY

BY: _____ **DATED:** 3-16-22

DATA PRIVACY AND SECURITY PLAN

In hosting Protected Data, Contractor and/or any of its subcontractors, affiliates or third parties that may receive, collect, store, record or display any Protected Data, shall maintain a Data Security and Privacy Plan that includes the following elements:

Hardware and infrastructure behind the service:

Application services provided are distributed between two data centers. The servers sit behind enterprise load-balancers that are connected to redundant, high-speed network connections.

The co-location data centers reside within the United States located in Denver, CO and Secaucus, NJ. Both co-location data centers provide Tier 3 level features including emergency backup environmental systems for continuous 24 x 7 operation.

Security utilized to protect customer data:

Customer Segregation:

Customers are logically segregated from one another ensuring only authorized personnel have access to data.

Encryption:

All end-user access to information stored in the Service is encrypted and transmitted via HTTPS. All authenticated access is protected by SSL certificate issued by a Certificate Authority

Firewalls and Intrusion Detection/Intrusion Prevention system is used to protect the Service network.

Diligent Employees with access to the underlying infrastructure is limited to authorized personnel only through VPN to create secure and encrypted connections.

Disaster Resilience and Recovery:

Geographical Redundancy

The Service's servers are housed at two geographically separated sites within the United States. one outside Denver, Colorado and one in a Secaucus, NJ co-location centers. Each site maintains copies of all production data. Each site functions in an active/warm standby environment and capable of providing the Service from either location. Administrative access is provided via VPN.

Staff is geographically dispersed, providing resilience in staff's ability to provide customer support.

Hardware Redundancy:

Each site has mirrored servers in an active/warm standby configuration. Production data is stored at both sites. The data centers have multiple internet backbones into both centers, ensuring resilience should there be a major internet backbone outage. The data centers also have backup power in the form of batteries for short-term problems and diesel generators for longer-term problems.

Monitoring:

Monitoring software is used within the production environment to monitor on a 24/7 basis and alert engineering and production operations staff.

Backups:

Full backups are stored and retained for 14 days. Access to the backups is limited to authorized and mission-critical staff only.

Disaster Recovery:

IT staff maintains a Business Continuity & Disaster Recovery plan and associated processes necessary to restore service.

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;

   The program is designed to store information, including student PII, which is used by the district's or BOCES Board.

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;

   Customer sites are logically segregated from one another, ensuring only authorized personnel have access to data. Diligent has imposed on its personnel and subcontractors substantially similar data protection obligations as are imposed on Diligent under the Education Law 2-d Agreement. Diligent is responsible for the acts and omissions of its personnel and subcontractors that perform Diligent's obligations under the Education Law 2-d Agreement.

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

   Diligent Corporation will destroy or return any data in its possession upon the expiration of the contract.

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

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

   All data resides within servers stored in the United States.

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. Except for authorized representatives of the third party contract to the extent they are carrying out the contract, 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.