This Education Law 2-d Rider ("Rider") is dated October 16, 2020, and is attached to and made part of the BoardDocs End User Agreement, dated October 27, 2015, by and between Albany-Schoharie-Schenectady-Saratoga BOCES ("Client") whose principal place of business is 900 Watervliet-Shaker Road, Albany, NY 12205 and Diligent Corporation (hereinafter "Diligent"), a Delaware corporation, whose principal place of business is 1111 19th Street NW, 9th Floor, Washington, DC 20036 ("the Agreement"). All capitalized terms not defined herein shall have the meanings ascribed to them in the Agreement. Each of Client and Diligent are a "Party" and are together the "Parties.

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, the Client, and certain third-party contractors who contract with the Client shall take certain additional steps to reasonably secure such data. These steps include enacting and complying with a Parents' "Bill of Rights" relative to protected data and 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 Client's Parents' Bill of Rights, thereby signifying that the third-party contractor will, to the extent required by law, comply with such Parents' Bill of Rights. The Parties agree that the Agreement is subject to the requirements of Education Law 2-d.

In order to comply with the mandates of Education Law 2-d, and notwithstanding any provision of the Agreement between Diligent and Client to the contrary, Diligent agrees as follows:

Diligent will treat "Protected Data" (as defined below) that is uploaded to the Service 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 Diligent uses to protect its own confidential data, designed to prevent the unauthorized dissemination or publication of Protected Data to third parties. Diligent 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. Diligent shall not use Protected Data for any purpose other than to fulfill its obligations under the Agreement. All Protected Data shall remain the property of the disclosing party. As more fully discussed below, Diligent shall have in place reasonable internal controls designed to protect the confidentiality of Client's Protected Data in accordance with all applicable laws and regulations, including, but not limited to, CIPA, FERPA and HIPAA, if applicable.

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

> "Personally identifiable information" from student records of Client and/or its Participants as that term is defined in §99.3 of the Family Educational Rights and Privacy Act (FERPA) that is uploaded to the Service,
>
> -AND-
>
> Personally identifiable information from the records of Client and/or its Participants 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 that is uploaded to the Service.

Diligent and/or any of Diligent's subcontractors, affiliates, or agents that may receive, collect, store, record or display any Protected Data shall comply with, to the extent applicable, New York State Education Law § 2-d. As applicable, Diligent agrees to comply with the data security and privacy plan identified below. To the extent required under New York State Education Law § 2-d, subsection 6(c), Diligent shall promptly reimburse Client for the full cost of notifying a parent, eligible student, teacher, or principal of an

unauthorized release of Protected Data by Diligent. Following termination or expiration of this Agreement, Diligent shall return Protected Data to Client by secure transmission, in accordance with Section 6 (Termination) of the Agreement.

Data Security and Privacy Plan

In hosting Protected Data, Diligent shall, and shall reasonably cause its subcontractors, affiliates, or third parties that may receive, collect, store, record or display any of Client's Protected Data, to comply with the Data Security and Privacy Plan set forth below:

1. Diligent shall incorporate the requirements of the Parents' Bill of Rights (as set out below) for data security and privacy, to the extent that any of the provisions in the Bill of Rights applies to Diligent's possession and use of Protected Data pursuant to this Agreement.

2. An outline of how applicable state, federal, and local data security and privacy contract requirements will be implemented over the life of the contract, consistent with Diligent's policy on data security and privacy.

3. An outline of the measures taken by Diligent to secure Protected Data and to limit access to such data to authorized employees and third parties.

4. An outline of how Diligent will use industry standards with respect to data storage, privacy, and protection, including, but not limited to encryption, firewalls, passwords, protection of off-site records, and limitations of access to stored data to authorized employees and third parties.

5. An outline of how Diligent will reasonably ensure that any subcontractors, persons, or entities with which Diligent will share Protected Data, if any, will abide by the requirements of Diligent's policy on data security and privacy, and the contractual obligations with respect to Protected Data set forth herein.

DATA SECURITY AND PRIVACY PLAN

In hosting Protected Data, Diligent 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.

An executed copy of Client's Parent's Bill of Rights is attached hereto as Exhibit A and incorporated herein.

EXHIBIT A

PARENTS' BILL OF RIGHTS
FOR DATA SECURITY AND PRIVACY

Albany-Schoharie-Schenectady-Saratoga BOCES (Capital Region BOCES), in recognition of the risk of identity theft and unwarranted invasion of privacy, affirms its commitment to safeguarding student personally identifiable information (PII) in educational records from unauthorized access or disclosure in accordance with State and Federal law. BOCES establishes the following parental bill of rights:

- Student PII will be collected and disclosed only as necessary to achieve educational purposes in accordance with State and Federal Law.
- A student's personally identifiable information cannot be sold or released for any marketing or commercial purposes by BOCES or any a third-party contractor. BOCES will not sell student personally identifiable information and will not release it for marketing or commercial purposes, other than directory information released by BOCES in accordance with BOCES policy.
- Parents have the right to inspect and review the complete contents of their child's education record (for more information about how to exercise this right, see 5500-R).
- State and federal laws, such as NYS Education Law §2-d and the Family Educational Rights and Privacy Act, protect the confidentiality of students' personally identifiable information. 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.
- A complete list of all student data elements collected by the State Education Department is available for public review at http://nysed.gov/data-privacy-security or by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.
- Parents have the right to have complaints about possible breaches and unauthorized disclosures of student data addressed. Complaints should be directed to the Data Protection Officer, (518) 464-5139, DPO@neric.org, **Capital Region BOCES, 900 Watervliet-Shaker Rd., Albany NY 12205.** Complaints can also be directed to the New York State Education Department online at http://nysed.gov/data-privacy-security by mail to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234 or by email to privacy@mail.nysed.gov or by telephone at 518-474-0937.
- Parents have the right to be notified in accordance with applicable laws and regulations if a breach or unauthorized release of their student's PII occurs.
- Parents can expect that the Client workers who handle PII will receive annual training on applicable federal and state laws, regulations, Client's policies and safeguards which will be in alignment with industry standards and best practices to protect PII.
- In the event that BOCES engages a third-party provider to deliver student educational services, the contractor or subcontractors will be obligated to adhere to State and Federal Laws to safeguard student PII. Parents can request information about third party contractors by contacting the Data Protection Officer, (518)-464-5139, DPO@neric.org, 900

Watervliet-Shaker Rd., Albany NY 12205, or can access the information on BOCES' website https://www.capitalregionboces.org/.

Supplemental Information Regarding Third-Party Contractors:

In the course of complying with its obligations under the law and providing educational services, Client 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 Client 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;

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;

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

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.

Third Party Contractors are required to:

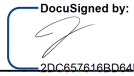
1. Provide training on applicable federal and state laws governing confidentiality to any officers, employees, or assignees who have access to Protected Data;
2. Limit internal access to Protected Data to those individuals who have a need to access them in order to fulfill Diligent's obligations under the Agreement.
3. Not use Protected Data for any other purpose than those necessary for Diligent to fulfill its obligations under the Agreement;
4. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of Protected Data;
5. Use encryption technology to protect Protected Data while in motion or in its custody from unauthorized disclosure as specified in Education Law §2-d;
6. Notify Client of any breach of security resulting in an unauthorized release of Protected Data, without unreasonable delay;
7. Provide a data security and privacy plan outlining how all applicable state, federal and local data security and privacy contract requirements will be implemented over the life of the Agreement;
8. Provide a signed copy of this Bill of Rights to Client thereby acknowledging that they are aware of and agree to abide, to the extent applicable to Diligent's obligations, 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.

Diligent hereby acknowledges that it is aware of and agrees to abide, to the extent applicable to Diligent's obligations, by the terms of this Bill of Rights. A copy of this signed document must be made a part of the Diligent's data security and privacy plan.

[Signature Page Follows]

DILIGENT CORPORATION

SIGNATURE: 

NAME: John Van Arsdale

TITLE: General Counsel