SCHEDULE E
EDUCATION LAW 2-d RIDER

New York State Education Law 2-d was enacted in 2014 to address concerns relative to securing certain personally identifiable information. In order to comply with the requirements of Education Law 2-d, educational agencies and certain third-party contractors who contract with educational agencies must take certain additional steps to secure such data. These steps include enacting and complying with a Parents' "Bill of Rights" relative to protected data, ensuring that each third-party contractor has a detailed data privacy plan in place to ensure the security of such data, and that each third-party contractor sign a copy of the educational agency's Parents' Bill of Rights, thereby signifying that the third-party contractor will comply with such Parents' Bill of Rights. This Agreement is subject to the requirements of Education Law 2-d and Follett School Solutions, Inc. (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 student data, student demographics, scheduling, attendance, grades, health and discipline tracking, and all other data reasonably considered to be sensitive or confidential data by ESBOCES and/or participating school districts. Protected Data also includes any information protected under Education Law 2-d including, but not limited to:

> "Personally identifiable information" from student records of ESBOCES and/or participating school districts as that term is defined in § 99.3 of FERPA,
>
> -AND-
>
> Personally identifiable information from the records of ESBOCES and/or participating school districts relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§3012-c and 3012-d.

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any Protected Data shall comply with New York State Education Law § 2-d. As applicable, Contractor agrees to comply with ESBOCES' policy(ies) on data security and privacy. Contractor shall promptly reimburse ESBOCES and/or participating school districts for the full cost of notifying a parent, eligible student, teacher, or principal of an unauthorized release of Protected Data by Contractor, its subcontractors, and/or assignees. In the event this Agreement expires, is not renewed or is terminated, Contractor shall return all of ESBOCES' and/or participating school districts' data unless otherwise provided, including any and all Protected Data, in its possession by secure transmission.

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any of ESBOCES' and/or participating school districts' Protected Data, shall maintain a Data Security and Privacy Plan which includes the following elements:

1. Specifies the administrative, operational and technical safeguards and practices in place to protect personally identifiable information that Contractor will receive under the contract;
2. Demonstrates Contractor's compliance with the requirements of Section 121.3 of Part 121;
3. Specifies how officers or employees of the Contractor and its assignees who have access to student data, or teacher or principal data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;
4. Specifies how Contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;
5. Specifies how Contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the educational agency;
6. Specifies whether Protected Data will be returned to ESBOCES and/or participating school districts, transitioned to a successor contractor, at ESBOCES' and/or participating school districts' option and direction, deleted or destroyed by the Contractor when the contract and/or the Agreement to Terms is terminated or expires.

Pursuant to the Plan Contractor will:

1. Have adopted technologies, safeguards and practices that align with the NIST Cybersecurity Framework referred to in Part 121.5(a);
2. Comply with the data security and privacy policy of ESBOCES; Education Law § 2-d; and Part 121;
3. Have limited internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services;
4. Have prohibited the use of personally identifiable information for any purpose not explicitly authorized in this contract;
5. Have prohibited the disclosure of personally identifiable information to any other party without the prior written consent of the parent or eligible student:
    a. except for authorized representatives such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with state and federal law, regulations and its contract with the educational agency; or
    b. unless required by statute or court order and Contractor has provided a notice of disclosure to the department, district board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.
6. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in our custody;
7. Use encryption to protect personally identifiable information in its custody while in motion or at rest; and

or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

In the event Contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the third-party contractor by state and federal law and contract shall apply to the subcontractor.

Where a parent or eligible student requests a service or product from a third-party contractor and provides express consent to the use or disclosure of personally identifiable information by the third-party contractor for purposes of providing the requested product or service, such use by the third-party contractor shall not be deemed a marketing or commercial purpose prohibited by the Plan.

Contractor's signature below shall also constitute an acknowledgement, acceptance, and signature of ESBOCES' or participating school district's Parents' Bill of Rights.

NAME OF CONTRACTOR: FOLLETT SCHOOL SOLUTIONS, INC.

BY: Pat
Patrick F. Sullivan

DATED: 4-2-2021

DATA PRIVACY AND SECURITY PLAN

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

Vendor's DATA SECURITY AND PRIVACY PLAN is as follows:

Follett Data Security

Follett is committed to data security and supporting our customers' data privacy needs. As student data collection evolves, Follett continues to provide and enhance the necessary levels of security to ensure your student information is secure and private in our learning management and educational systems.

Protection of individual sensitive and personally identifiable information (i.e. PII) is a priority for Follett. To ensure compliance with all applicable privacy legislation Follett has established policies and processes that focus on the protection of all potentially sensitive customer data. Follett has invested in technologies that support the protection and provide security of data while in transit or at-rest.

Follett's Pledge of Student Privacy

Follett is proud to be one of the first signers of the national Student Privacy Pledge (https://studentprivacypledge.org) regarding the collection, maintenance, and use of student personal information. The pledge states: "School service providers take responsibility to both support the effective use of student information and safeguard student privacy and information security." Follett takes the signing of Student Privacy Pledge seriously and strives to go above and beyond the privacy constructs defined within.

Destiny

- The data model consists of a single database; data does not need to be replicated to other data stores.
- Each Destiny district has a separate physical database file.
- Security rules are applied universally to each database instance.
- The database is not accessible from outside the data center firewall in case the Destiny product is housed at the Follett-managed data center.
- The database is not directly accessible via the public internet.
- All access to the database is managed through the application, and data is only visible to users with specific rights and permissions.
- Destiny is routinely tested against attacks using automated acceptance testing, such as exercises and sample data intended to uncover SQL injection vulnerabilities. Authentication methods are exercised through automated unit tests to validate that data access is restricted to users with the appropriate permissions.
- Destiny also has multiple levels of supported data security

Follett eBooks and Security

Data Security

All data is securely transmitted over the HTTPS protocol. This includes page content, images, fonts, and user data. All data is then stored into an encrypted data store on the local machine, inside a directory that only that user (and root) has access to. The encryption key to unlock the data is generated locally at the time of the data store creation and stored in the system user's encrypted local store (ELS). Only a combination of our application store, separate from the main encrypted data store, with its own encryption key stored in the ELS. When the book is removed by the user via Follett Digital reader, its data store is deleted from the local file system, which includes all content, imagery, and fonts.

DRM

We encrypt each book with 128bit AES encryption, and every book has its own unique key. In addition to encrypting the book, we have a voucher mechanism that is also encrypted using 128bit AES encryption and ensures the content is locked to the specific machine it was downloaded to.

Follett eReader

Follett uses a proprietary conversion and encryption process that our Follett readers have been designed specifically to utilize.

About Our Data Center

The Data Center where Follett houses and manages its servers is an approximately 3,000 square-foot, raised-floor facility. Physical access to the data center is controlled by a card proximity reader. Only individuals with a role that requires access to the data center are permitted in the raised floor area. Access to the mechanical space is similarly controlled. A camera system has been installed at the doors to the data center to record entrance and exit to the raised floor and mechanical space. Procedures are in place to log the access to the data center.

Data Center contained server access is similarly controlled with secured access by Follett employees as well as approved designated third party vendors / systems (i.e. development consultants, hardware vendors, SIF agents).

Contact Us

Follett is committed to helping our customers demonstrate the privacy and security of their student data. Our security features are designed to provide physical and digital security and empower districts to develop, enact, and enforce their privacy policies. For more information about our data security, please contact us.

An executed copy of ESBOCES' Parent's Bill of Rights is attached hereto and incorporated herein.

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;

of users is done through the process of sharing a limited amount of personally identifiable information for that purpose.

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;

   A: Follett provides security training annually to its employees, recorded in their training dashboard, and intermittent touch points throughout the year. In addition, staff has Ethics training which includes data confidentially handling. Follett utilizes the KnowBe4, https://www.knowbe4.com/, platform training.

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

   A: Securely transfer data to Eastern Suffolk BOCES, or a successor contractor at Eastern Suffolk BOCES's option and written discretion, in a format agreed to by the parties.

   Securely delete and destroy data.

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

A: Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to your district's Associate Superintendent for Educational Services, or in writing to the 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.

   A: The Data Center located in Lisle, IL where Follett houses and manages its servers is an approximately 3,000 square-foot, raised-floor facility. Physical access to the data center is controlled by a card proximity reader. Only individuals with a role that requires access to the data center are permitted in the raised floor area. Procedures are in place to log the access to the data center.

   Follett utilizes third party certified data centers: Azure cloud

   https://azure.microsoft.com/en-us/overview/trusted-cloud/compliance/

   Contractor hosted solution is in Evoque: https://www.datacenters.com/evoque-solutions-chicago-ch1-lisle

   Follett is planning on migrating the Destiny application to the Azure cloud environment 2020-2021. Microsoft maintains a "No Standing Access" policy on customer data. They have engineered their products so that many service operations are fully automated and only a small set of activities require human involvement. Access by Microsoft personnel is granted only when necessary for support or operations; access is carefully managed and logged, then revoked when no longer needed. Datacenter access to the systems that store customer data is strictly controlled via lock box processes. Microsoft will not have access to the Eastern Suffolk BOCES data

Third Party Contractors are required to:

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.