

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 BC Technologies Company d/b/a FinalForms (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.

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 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

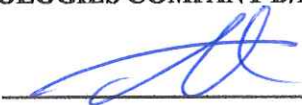
8. Not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

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.

BC TECHNOLOGIES COMPANY D/B/A FINALFORMS

BY:  _____

DATED: 4/15/2021

DATA PRIVACY AND SECURITY PLAN

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

DATA SECURITY AND PRIVACY PLAN

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

1. OVERVIEW

This Privacy Policy explains the nature of Vendor's collection, use, and disclosure of the data Authorized Users provide to Vendor when using the Licensed Product.

Vendor never sells the personal, aggregate or de-identified data Vendor collects from Vendor's users.

DEFINITIONS

Vendor provides data collection, data management, and communication tools for its clients, which includes school districts. Vendor provides access to its Licensed Product to Authorized Users.

1. For purposes of this Agreement, "Confidential Information" shall mean any information, in any form, oral, written, or electronic, about a current or former student of the District, including, but not limited to, "Education Records" and Personally Identifiable Information," as these terms are defined under the Family Educational Rights and Privacy Act of 1974, as amended, or as may be amended hereinafter ("FERPA"). Confidential Information SHALL include "Directory Information," as this term is defined under FERPA. Confidential Information shall include, without limitation, any information, in any form, oral, written, or electronic, about District student test data, test scores, grades, student records; District operations, activities, finances, passwords, databases, reports, processes, practices; former and current District consultants, personnel records, agreements, and any information protected under the Health Insurance Portability and Accountability Act of 1996, and any amendments thereto ("HIPAA"), or any other applicable Federal or State Law. Confidential Information shall not include information that is published, or otherwise in the public domain. Notwithstanding any language in this Agreement to the contrary, Confidential Information shall include Protected Data as defined in Schedule E, "Education Law 2-d Rider," of this Agreement.

2. For purposes of this Agreement, "Disclosure" shall have the definition given the term under FERPA: "to permit access to or the release, transfer, or other communication of personally identifiable information contained in education records, by any means, including oral, written, or electronic means, to any party except the party identified as the party that provided or created the record." The definition of Disclosure shall include permitting access to, or the release, transfer, or other communication of any Confidential Information, by any means, including, without limitation, oral written or electronic.

CHANGES

If there are any material changes to this Privacy Policy, Vendor will provide prior written notice to Customer and Authorized Users and comply with the terms for amendment contained in the License Agreement.

SCOPE

This Privacy Policy is effective with respect to any data that Vendor has collected about and/or from Authorized Users according to this License Agreement.

2. DATA & ACCOUNTS

DATA COLLECTED FOR AND BY SCHOOL DISTRICTS

An Authorized User may supply data to Vendor, as required by his/her Participant Vendor does not require an Authorized User to supply it with data. Individuals using the Licensed Product provided by Vendor are responsible for ensuring that they meet the qualifications for the status of Authorized User, as determined by their Participant/School District. Authorized Users are responsible for ensuring the accuracy and completeness of all information supplied to Vendor. An Authorized User may access and correct personally identifiable information through use of the Licensed Product at any time.

DELETING A FINALFORMS ACCOUNT

Authorized Users desiring to delete their accounts or otherwise remove data they have supplied to Vendor must contact their Participant/School District.

3. AUTHORIZED USER DATA IN LICENSED PRODUCT FINALFORMS

DATA AUTHORIZED USERS PROVIDE TO VENDOR

Through using the Licensed Product provided by Vendor, an Authorized User may supply Vendor with data, including but not limited to the Authorized User's name, email address, phone number, IP address, operating system, gender, location, birth date, service usage history, and other demographic information. By supplying Vendor this data, an Authorized User consents to his/her data being collected, used, disclosed, and stored by Vendor, as described in this License Agreement and this Privacy Policy. Authorized Users may log in to Vendor's Licensed Product at any time to correct or update any data held anywhere within their account.

INFORMATION FROM AUTHORIZED USER'S /CUSTOMER'S USE OF THE LICENSED PRODUCT

Vendor may gather information about how and when Authorized User or Customer uses the Licensed Product, store it in log files associated with Authorized User's account, and link it to

other information Vendor collects about Authorized User. This information may include, for example, Authorized User's IP address, time, date, browser used, and actions within the Licensed Product.

COOKIES AND TRACKING

When Authorized User or Customer uses the Licensed Product, FinalForms, Vendor may store "cookies" or "scripts," which are strings of code, on Authorized User's /Customer's computer. Vendor uses those cookies to collect information about Authorized User's /Customer's visit and Authorized User's / Customer's use of Vendor's Licensed Product. Authorized User /Customer may turn off cookies that have been placed on Authorized User's /Customer's computer by following the instructions on Authorized User's /Customer's browser, but if Authorized User blocks cookies, it may be more difficult to use some aspects of the Licensed Product.

USE AND DISCLOSURE OF DATA SUPPLIED BY AUTHORIZED USERS

Vendor may use and disclose the data supplied by an Authorized User for purposes such as:

1. To promote the use of our Licensed Product. For example, we may calculate the average amount of time an Authorized User spends completing a task within the service and create a promotion such as, "On average, users spend less than 5 minutes signing forms."
2. To provide, support, and improve the services we offer.
3. To communicate with you about your account and provide customer support.
4. To enforce compliance with this License Agreement and applicable law.
5. To protect the rights and safety of Participants/School Districts, our Authorized Users, and Vendor.
6. To meet legal requirements, such as complying with court orders, valid discovery requests, valid subpoenas, and other appropriate legal mechanisms.
7. To provide information to representatives and advisors, like attorneys and accountants, to help Vendor comply with legal, accounting, or security requirements.
8. To prosecute or defend a court, arbitration, or similar legal proceeding.
9. To provide suggestions to Customer.

PUBLIC INFORMATION AND THIRD PARTIES

Vendor will not make publicly available the individual data an Authorized User supplies it by

using the Licensed Product. Vendor will not use any behavioral information to provide targeted advertising to Authorized Users. Vendor will not collect, use, or share behavioral information for any purpose beyond authorized educational or school purposes, or as authorized by the Authorized User. Vendor does not limit a Participant's/School District's use of the data that an Authorized User supplies Vendor through use of the Licensed Product.

In the event of a merger or acquisition by another entity, Vendor will not provide an Authorized User's personal information to such successor entity unless the entity agrees to the "Student Privacy Pledge" as set forth by the "Future of Privacy Forum" and the "Software and Information Industry Association,": <https://studentprivacypledge.org/privacy-pledge/> Vendor will not share Authorized User information with any vendor that would be used to deliver the Licensed Product for or on behalf of Vendor, unless the vendor agrees to the commitments of the aforementioned "Student Privacy Pledge," with respect to student personal information, or unless use of the vendor is authorized by the relevant educational institution/agency or Authorized User.

LINKS TO THIRD PARTY WEBSITES

The **Licensed Product** may include links to other websites, whose privacy policies may differ from Vendor's. If Authorized Users submit information to any of those websites, Authorized Users' information is governed by their privacy policies. Vendor encourages Authorized Users to carefully review the privacy policy of any website Authorized Users visit.

4. SECURITY

NOTICE OF BREACH OF SECURITY

If a security breach causes an unauthorized intrusion into Vendor's system that materially affects Customer, then Vendor will notify Customer as soon as possible and later report the action that was taken in response to the intrusion and Vendor shall promptly reimburse ESBOCES and/or its Participants for the full cost of notifying a parent, eligible student, teacher, or principal of an unauthorized release of Protected Data by Vendor, its subcontractors, and/or assignees.

SAFEGUARDING DATA

Vendor's FinalForms accounts require a username and a password to log in. Authorized Users must keep Authorized User's username and password secure. Because each Authorized User's password is so sensitive, account passwords are encrypted. Vendor cannot resend forgotten passwords. Vendor can allow an Authorized User to reset Authorized User's password if Authorized User provides the correct credentials.

Vendor maintains a comprehensive security program that is designed to protect the security, privacy, confidentiality, and integrity of Authorized Users' information against risks through the use of administrative, technological, and physical safeguards. Details about FinalForms' security program can be found at <http://final.publishpath.com/security>

CLOUD HOSTING SERVICES

By using the Licensed Product, Participant / Customer understands and consents to the collection, storage, processing, and transfer of Participant's / Customer's data to Vendor's cloud service hosting provider. The cloud service hosting provider will agree to and comply with all the terms and conditions of this License Agreement, including the terms and conditions of this Schedule E.

5. COMPLIANCE

Vendor regularly reviews Vendor's compliance with Vendor's Privacy Policy. If Vendor receives a complaint, Vendor responds to the Authorized User who made it. Customer may contact Vendor by using Vendor's online form. Vendor will provide ESBOCES with a report summarizing any complaints received by Vendor as they are received and addressed.

An executed copy of ESBOCES' Parent's Bill of Rights 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;

FinalForms provides a service that enables school districts to manage student data. FinalForms shall only use student data to provide the service, as permitted under the terms of its agreement with ESBOCES.

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;

All FinalForms' subcontractors, persons or entities used by FinalForms shall be limited in their use of student data to only those uses for which FinalForms is authorized pursuant to its agreement with ESBOCES. FinalForms shall monitor subcontractors, persons or entities used by FinalForms for compliance with this condition.

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

Upon the expiration of the agreement, all data shall be returned to the school district and/or ESBOCES, as directed by the school district.

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

Challenges to the accuracy of student data shall be registered with the relevant school district, using the contact information found in such district's Parent's Bill of Rights. The school district may then contact FinalForms for the matter to be addressed.

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.

FinalForms is hosted in its entirety on FinalForms infrastructure on Amazon Web Services ("AWS") EC2 and S3 instances, within the United States. AWS infrastructure is designed and managed according to the highest standards for security and data protection, including SOC 1, 2, 3, PCI DSS Level 1, ISO 27001, FIPS 140-2, and more, as well as military-grade physical controls. Data will be secured with SSL encryption.

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.