

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 YellowFolder, 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 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.

YellowFolder, LLC

BY: Lessa Tyler

DATED: 5/27/21

DATA PRIVACY AND SECURITY PLAN

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

Privacy Policy

Statement:

YellowFolder LLC is committed to protecting your privacy. YellowFolder LLC has created this privacy statement in order to demonstrate our firm commitment to your privacy.

Collection of your Personal Information:

YellowFolder collects personal information, such as e-mail address, name, home or work address or telephone and fax number(s) (collectively, "User Information"), and stores personal information on students and staff of K-12 education entities, including information such as student records, personnel records and other school forms and materials containing private information related to both students and staff members (collectively, "School Information"; User Information and School Information are collectively referred to as "Information"). YellowFolder has taken the commercially reasonable steps to ensure that Information is kept confidential at all times. YellowFolder processes and uses School Information exclusively for educational purposes and to fulfill contractual agreements between the respective schools and districts that own the School Information.

These Steps Include:

- YellowFolder enforces strict, limited access to Information databases for YellowFolder's internal purposes.
- YellowFolder communicates this privacy statement to all YellowFolder employees and subcontractors, provides training on federal and state law governing information confidentially, and requires strict compliance with data protection and security requirements.
- YellowFolder has not, and will not, sell, rent, disseminate or disclose any School Information or User Information on the YellowFolder system to any other company or organization for any purpose.
- YellowFolder provides each client education entity ("Education Entity") with the ability to receive electronic copies of any and all data related to such Education Entity kept on the YellowFolder system at all times. YellowFolder also will provide authorized staff of such Education Entity with the ability to review (and potentially, correct) data maintained on the YellowFolder system and related to their tenure with such Education Entity, provided that such authorized staff member follows the laws, regulations and rules for accessing such School Information via formal channels established within the client Education Entity and the legal jurisdictions where it is located.
- YellowFolder retains each Education Entity's School Information on the YellowFolder system based on retention schedules approved by such Education Entity. Upon a termination of all services with an Education Entity, YellowFolder provides the Education

Entity with the ability to receive electronic copies of all records and data maintained on the YellowFolder system, and permanently removes and destroys all data related to such Education Entity from the YellowFolder system.

- YellowFolder communicates via mail, e-mail or other online delivery devices unless you tell us not to. If you believe you are receiving our communications in error or no longer desire to receive these communications, please inform YellowFolder and we will remove your name from our mailing lists.
- YellowFolder will require any successor entity to YellowFolder to adhere to the terms and conditions of this privacy statement, or to provide advance written notice to all the then-current Education Entities using the YellowFolder system of any limitations to this privacy statement, and, in the event that limitations are forthcoming, a reasonable period of notice regarding such privacy statement changes to allow the Education Entity time to seek an alternative storage repository for its data.

Links:

The Site contains links to other websites. Please note that when you click on one of these links, you are moving to another website. We encourage you to read the privacy statements of these linked sites as their privacy policy may differ from ours.

Cookies and Osano:

YellowFolder uses data governance and compliance services provided by Osano ([Osano Privacy Policy](#)) that use JavaScript and cookies. This service may use cookies to collect information for analytics. Cookies are very small text files stored on your computer by your web browser. You may refuse the use of cookies by selecting the appropriate settings on your browser. If cookies are refused, you will still be able to use the Site, and anonymous data will still be collected in our internal transaction logs. By accepting cookies, you consent to the processing of data in the manner and for the purposes set out in this privacy statement.

Security of your Personal Information:

YellowFolder is committed to protecting the security of your Information. We use security technology and procedures to help protect your Information from unauthorized access, use or disclosure in compliance with state, federal and local data security and privacy requirements. We store the Information you provide on redundant computer systems located in controlled facilities in the United States of America. When transmitting and storing highly confidential information such as School Information, we protect it through the use of encryption by industry standard Secure Sockets Layer ("SSL") technology using AES 256-bit encryption so that it cannot be read even if it is wrongly intercepted.

Breach Response:

A breach is defined as an incident where sensitive, protected, or confidential personal information and personal data has potentially been accessed, stolen, or used without authorization. In the event of a data breach, YellowFolder will follow the minimum guidelines or policies formally adopted prior to such breach by the applicable state agency or authority

governing the District in responding to such data breach.

Changes:

YellowFolder reserves the right to change, modify, add or remove portions of this privacy statement at any time, but will alert you on the Site that changes have been made by indicating on the privacy statement the date it was last updated. When you visit the Site you are accepting the current version of this privacy statement as posted on the Site at that time. We recommend that users re-visit this privacy statement on occasion to learn of any changes. In the event that YellowFolder limits the privacy rights of client Education Entities or their authorized staff in any manner, YellowFolder will provide a notice on the Site at the time of login notifying of changes to this privacy statement.

Contact Information:

YellowFolder welcomes your comments regarding this privacy statement. If you believe that YellowFolder has not adhered to this privacy statement, please contact YellowFolder by telephone, e-mail or postal mail.

YellowFolder LLC
P.O. Box 3068
McKinney, TX 75070
[\(214\) 431-3600](tel:2144313600)
support@yellowfolder.com
Updated: 2/11/2021

**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;

Student and/or staff data is used to create metadata tags to store student and staff personnel records on the YellowFolder system. The metadata tags are used exclusively by the district in question and the data is not shared with other YellowFolder customers.

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;

YellowFolder shall be subject to the data protection provisions of this agreement and laws passed by the State of New York.

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

YellowFolder permanently destroys all metadata tag information upon expiration or termination of an applicable school district's contract with YellowFolder.

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

YellowFolder only uses the student information to create a filing system for the individual student's or staff's records. It is administrative use only. If the data is deemed inaccurate, YellowFolder will amend the administrative use. This has not been a practical concern to date.

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 YellowFolder data is stored in an encrypted methodology on industry-standard digital platforms housed in a professionally staffed and administered data center in Dallas, Texas.

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.