

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 Illuminate Education, 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 FIRE ISLAND UNION FREE SCHOOL DISTRICT (the "District") and Contractor 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 the District's 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 the District. Protected Data also includes any information protected under Education Law 2-d including, but not limited to:

"Personally identifiable information" from student records of the District as that term is defined in § 99.3 of FERPA,

-AND-

Personally identifiable information from the records of the District 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 District policy(ies) on data security and privacy. Contractor shall promptly reimburse the District 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 the District's 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 the District's 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 the District, transitioned to a successor contractor, at the District's option and direction, deleted or destroyed by the Contractor when the contract 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 the District; 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.

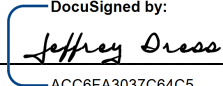
In the event Contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the third-party contractor by state and federal law and contract shall apply to the subcontractor.

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 the District's Parent Bill of Rights.

NAME OF PROVIDER: ·

ION, INC.

BY:  **DATED:** 8/25/2020
ACC6FA3037C64C5...

Effective Dates: July 1, 2020 to June 30, 2021

DATA PRIVACY AND SECURITY PLAN

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



Data Security & Privacy Plan

Illuminate is a web-based “all-the-data” system used by K-12 schools and districts to access student data. Teachers or administrators login to Illuminate and view student demographic and achievement data. Data is the primary element of the system and, as such, data security is paramount to Illuminate. This document will explain how Illuminate protects and values all of the data being utilized through the Illuminate systems.

Family Education Rights and Privacy Act (FERPA)

Illuminate adheres to all rules and regulations related to the protection of confidential student information as described in FERPA and District student confidentiality Board Policies. Illuminate’s extensive permissions system ensures that staff members can only access features and student records appropriate to their positions.

Permissions

Illuminate has implemented a comprehensive permission system that allows clients to establish precise access rights over software features and district data. This includes field-level permissions for sensitive data. All permissions are managed through an easy-to-use online web interface. The permission structure in Illuminate is paramount in enforcing FERPA compliance.

Data Access

User access via the web UI

Only users who have been authorized by the school district may login to the Illuminate system. Illuminate offers third party authentication (Active Directory, Google, etc.) integration options to clients who are leveraging the tools in order to bolster login security. All authorized users are provisioned their own individual account, and must provide appropriate credentials with every login. Additionally, users are automatically logged out of the system after a period of inactivity.

Direct database access

At the client’s request, direct read-only access to the Illuminate database can be granted to specific administrative users. This read-only access provides access only to the client database. All data is transmitted via SSL. The database user is given specific credentials to login to the database and access to the database is restricted to a client-specified IP address.

API access

Illuminate offers an open API to external parties at the request of clients. Prior to establishing the API access, the external party’s data usage plan is evaluated by Illuminate staff. All API consumers are vetted by Illuminate. Once an API partner has been provided secure API access, the actual access to a district’s installation is controlled by the district. API access is controlled by two levels of security -- first with API consumer tokens, and second with client administered and permissioned user access controls.

SFTP file transfers

Where routine file transfers are necessary for data imports and exports, only authorized users are granted restricted access to an Illuminate SFTP server. Secure FTP is used to ensure that sensitive data is encrypted in transit.

Software Security

All Illuminate data is stored securely and encrypted during transmission. The security at the software level includes secure access to the Illuminate API, single tenancy to ensure data privacy across clients, and transport layer security.

Secure API Access

API access is controlled by two levels of security -- first with API consumer tokens, and second with client administered and permissioned user access controls. Every time data is accessed via the API, both the consumer token and the client access keys are evaluated for security.

Single Tenancy

Each district's data is stored in its own dedicated database. Data is never co-mingled with data from other Illuminate clients. File transfers are also sent to district-specific locations to ensure that districts do not have visibility into each other's data.

Transport Layer Security

All Illuminate web traffic is encrypted over the wire via SSL. Firewalls are used to limit access to only essential services. Direct database access for district technical staff is managed by Illuminate, and all database traffic is also encrypted in transit via SSL.

Data Center and Cloud Provider

Illuminate products hosted in the Google Cloud Platform benefit from the same security precautions Google uses for its own products. Physical data centers include multi-layered security featuring camera and physical monitoring, credential scanning, and biometric checks.

<https://cloud.google.com/security/overview/whitepaper>

Illuminate also leverages a cloud-based data center at Amazon Web Services.

Google data center security includes:

- Key card access
- Biometric scanners
- Double mantrap entry
- 24x7x365 perimeter and interior recorded video surveillance
- 24x7x365 in-house security guards
- Locked server cabinets

Google data center certifications include:

- NIST SP 800–61
- ISO 50001

Backup and Disaster Recovery

Illuminate maintains both onsite and offsite backups for all client databases, allowing us to store and retrieve data anytime. Backups are shipped offsite nightly, and are encrypted at rest to prevent data theft. In the event of a catastrophic data center failure, we can retrieve data that is at most 24 hours old.

Audit Logs

Logging occurs at multiple levels within the system. We maintain a log in the system database that records data-changing operations. Page accesses can also optionally be recorded in a flat file showing the page accessed, the user performing the access, and the date/time of the access. Certain areas of the system, such as official student grades, also have their own logging features that track more detailed information about each transaction.

Conclusion

Illuminate believes in students and educators and takes the security of their data very seriously. Illuminate has gone to great lengths to ensure that data is secure physically, in all methods of data transit, and via the software application. Additionally, all Illuminate staff is trained on FERPA and the severe importance of data security. Users of the Illuminate system can use the system confidently, knowing that Illuminate deeply values data security.

Exhibit "A"
Fire Island UFSD
P.O. Box 428
Ocean Beach, NY 11770

PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

Pursuant to New York State 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, as defined by Education Law §2-d. This document contains a plain- English summary of such 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 educational records maintained by the Fire Island Union Free School District (Fire Island UFSD).
3. State and Federal Laws protect the confidentiality of personally identifiable student 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 New York State is available for review at the following website:
<http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx>

The list may also be made available by writing to:

Office of Information & Reporting Services New York State Education Department Room 863
EBA,
89 Washington Avenue
Albany, NY 12234

5. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to:

Loretta M. Ferraro, Superintendent Fire Island UFSD
P.O. Box 428
Ocean Beach, New York 11770
Ph: (631) 583-5626
Email: lferraro@fi.k12.ny.us

OR

Chief Privacy Officer
New York State Education Department 89 Washington Avenue
Albany, NY 12234
Email: CPO@mail.nysed.gov

6. Each contract with a third-party contractor which will receive 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 and principal data upon expiration of the agreement.
 - 4) If and how a parent, student, a student over eighteen years of age, 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, and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.
7. Third-party contractors are also 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 the Fire Island UFSD 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 the Fire Island UFSD thereby acknowledging that they aware of and agree to abide by this Bill of Rights.
8. 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.

Third-Party Acknowledgement

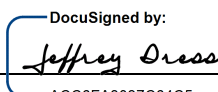
As a third-party contractor, I acknowledge that our contract with the Fire Island Union Free School District may necessitate the receipt of student data, and as such, requires adherence with NY State Education Law §2-d and the District's Parents' Bill of Rights for Data Privacy and Security. In this regard, we acknowledge our responsibility to adhere to the document as applicable to the services we provide, and have instituted processes to abide by same.

Name: Jeffrey Dress

Position: Vice President of Legal

Company: Illuminate Education, Inc.

Date: 8/25/2020

Signature: 
ACC6FA3037C64C5...

**Fire Island UFSD
P.O. Box 428
Ocean Beach, NY 11770**

**Supplemental Information for Ed Law 2-d
To be Posted on School District Website**

Pursuant to Education Law 2-d, following is the supplemental information required for the subscription to the vendor.

1. The exclusive purposes for which the student data or teacher or principal data will be used:
Please refer to the attached IE Data Security & Privacy Plan Document.

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:

Please refer to the attached IE Data Security & Privacy Plan Document.

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

The data is destroyed within 30 days of termination or non-renewal 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:

All requests for student data review, corrections, and/or copies by parents, legal guardians, and/or eligible students are redirected to the appropriate district personnel to address in accordance with district policies and applicable state laws.

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:

Please refer to the attached IE Data Security & Privacy Plan Document.