

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 Buncee 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 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.

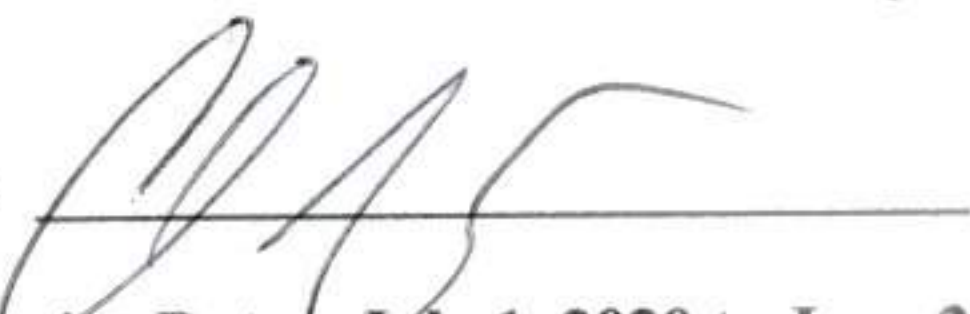
In the event Contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the third-party contractor by state and federal law and contract shall apply to the subcontractor.

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: <COMPANY> *Bunace LLC*

BY:



DATED:

08/18/2020

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.

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 are 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.

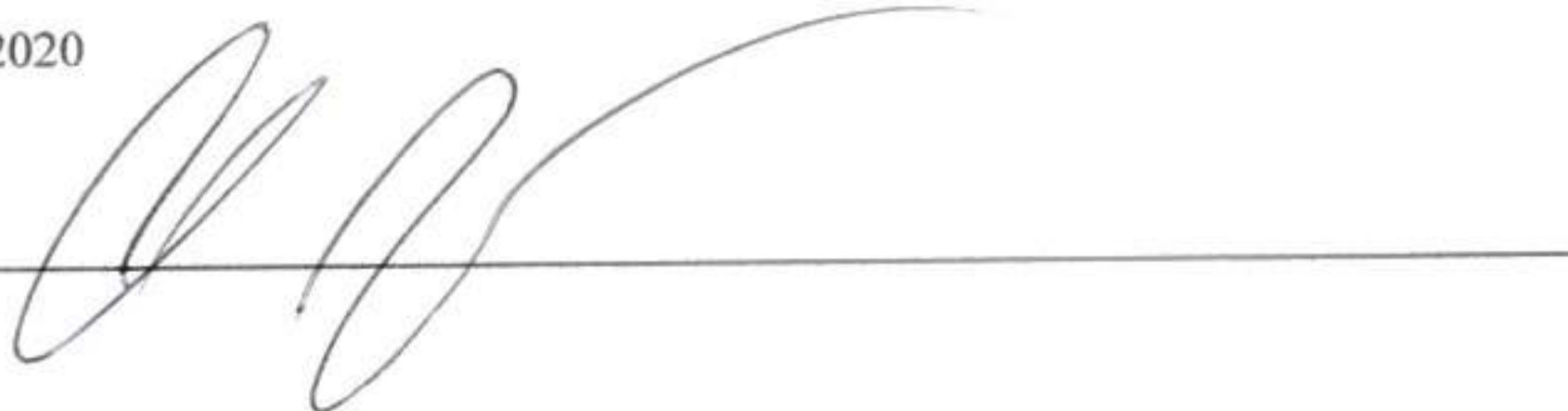
Name: Claire Cucchi

Position: Chief Operations Officer

Company: Buncee LLC

Date: 08/18/2020

Signature: _____



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:
The purpose of data processing is to allow Buncee to provide the requested Services to the District and perform the obligations under our Agreement. More specifically, the purpose of processing data is to enable school oversight and ensure appropriate structure and interaction within a school account on buncee.com. The processing of data enables the interaction, communication, creation and sharing within the classroom/school/district account; allows educators and/or administrators to monitor accounts, set permissions and deliver educational content; allows educators to differentiate and personalize a student's educational experience; and provides the admin-educator-student hierarchy within the account. Buncee requires data capture and use for the following reasons:

- **To confirm the identity of students and educators/administrators**
- **To provide educational services and content**
- **To allow subscribers to create and manage classes, personalize and differentiate instruction, and monitor and assess student progress**
- **To allow subscribers to monitor and safeguard student welfare**
- **To allow subscribers to set creation and sharing permissions and privacies schoolwide**
- **To inform existing subscribers about feature updates, site maintenance, and programs/initiatives (does not include subaccounts)**

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:

Buncee shall enter into a written agreement with any Subcontractors requiring the Subcontractor to uphold data protection practices that protect the District Data to the standard required by the Data Protection Laws (NYSED Law 2-D).

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

Buncee is a subscription based platform. Upon written notification from the District to terminate the account, Buncee shall promptly delete or return to the District all District Data in its possession or control, unless a student and/or parent has created an individual account with the Buncee and wishes to retain their account information.

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:

A parent, eligible student, teacher or principal may challenge the accuracy of the student, teacher or principal data by reaching out to Buncee at privacy@buncee.com.

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:

The following preemptive safeguards are in place to identify potential threats, manage vulnerabilities and prevent intrusion:

- All security patches are applied routinely
- Server access logging is enabled on all servers
- Fail2ban (an intrusion prevention software framework that protects servers from brute-force attacks) is installed on all servers and will automatically respond to illegitimate access attempts without intervention from Buncee's engineers
- Publicly accessible parameter for database instances is set to No, thereby disallowing any unauthorized access to the database servers
- SSH key-based authentication is configured on all servers

Buncee serves 100% of its traffic over HTTPS. The HTTPS you see in the URL of your browser means when you go to buncee.com, you're guaranteed to be getting the genuine Buncee website. With HTTPS in place, all interactions with Buncee will be undecipherable by an outside observer. They are unable to read or decode data. HTTPS is the same system that many sensitive websites, like banks, use to secure their traffic. This applies to all our custom Buncee for Schools & Districts urls too.

Buncee uses SSL security at the network level to ensure all information is transmitted securely. All content (i.e., photos, video, audio, and other content added to your Buncees) is encrypted at rest. All passwords are encrypted using bcrypt algorithm which is based on the secure blowfish encryption algorithm.

Account information is stored in access-controlled data centers operated by industry leading partners with years of experience in large-scale data centers. All user information is stored redundantly and backed up in geographically distributed data centers. We utilize multiple distributed servers to ensure high levels of uptime and to ensure that we can restore availability and access to personal data in a timely manner.

Buncee's application is hosted on cloud servers managed by Amazon Web Services and Digital Ocean, both of whom have rigorous physical measures to safeguard data, and are compliant with security standards including ISO 27001, SOC 2, PCI DSS Level 1, and FISMA. Data centers are conditioned to maintain atmospheric conditions at optimal levels. Personnel and systems monitor and control temperature and humidity at appropriate levels. These data centers are staffed 24/7/365 with onsite security to protect against unauthorized entry. Each site has security cameras that monitor both the facility premises as well as each area of the datacenter internally. There are biometric readers for access as well as at least two factor authentication to gain access to the building. Each facility is unmarked so as not to draw any additional attention from the

outside and adheres to strict local and federal government standards. Furthermore, physical access to our servers would not allow access to the actual data, as it is all protected via encryption.