# 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 Omega Labs Inc. dba Boom Learning (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 _____________________ (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"), and the Family Educational Rights and Privacy Act ("FERPA") 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, District shall use the tools provided to it by Contractor to export and delete all confidential information provided to Contractor. If for some reason Contractor is not able to avail itself of the self-help tools provided, it may contact Contractor to delete confidential information. Contractor will automatically delete confidential information on expired accounts pursuant to the Deletion schedule in its Privacy Policy. Deletion is irreversible and unrecoverable..

## 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.

Contractor will ensure that any subcontractors with whom it shares Protected Data are either (a) subject to obligations of confidentiality at least as protective as this agreement and receive annual training on their privacy and security obligations, or (b) are engaged under a contract under which they agree that they have no right of access to Protected Data stored in the subcontractors' cloud-based services.

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:** Omega Labs Inc. dba Boom Learning

**BY:** Mary E. Oemig **DATED:**

**CONTRACT TERMINATION DATE:**______________________________

# BOOM LEARNING DATA AND SECURITY PLAN
# NEW YORK SCHOOLS
## July 7, 2020 Revision (retroactively available)

**"Protected Data" subject to this Data and Security Plan.** Boom Learning collects personally identifiable information from students as that term is defined in §99.3 of FERPA. Specifically: (a) student task performance data (optional), (b) student first or last name or any combination or abbreviation thereof (optional) OR a psuedonomynous identifer OR other identifier selected by the school (at least one must be provided), (c) student email (optional).

**Applicability.** This Data and Security Plan shall apply to the Boom Learning employees, agents, subcontractors, and other contracted entities (**"Covered Persons"**) that may receive, collect, store, record or display any Protected Data from a New York entity subject to Education Law 2-d ("**Educators**"). Boom Learning shall ensure that Covered Persons are subject to agreements and commitments consistent with this Data and Security Plan. All Covered Persons must pass a background check.

**Parents' Bill of Rights.** Boom Learning agrees to incorporate into its agreements with the Education Entity, the provisions of the Education Entity's Parents' Bill of Right for data security and privacy, to the extent such provisions apply to the possession and use of Protected Data by Boom Learning.

**Exclusive Purposes for Data Use.** (1) To enable Educators to make, share, buy, sell and assign awesome digital educational resources (Boom Cards) that mostly grade themselves; and (2) to provide Educators with rapid student performance reporting to give you more time to teach students, intervene faster with those who need it, accelerate those who need it, and occasionally read a long privacy policy (or better yet a rollicking good book).

**Data Accuracy/Correction Practices.** Boom Learning provides Educators with the ability to delete data logs to remove data. Educators also have detailed log screens of student answers to evaluate the reliability of data reporting. Parents and students may challenge the accuracy of data by contacting their Educator. Educators may challenge the accuracy of data by contacting help@boomlearning.com and requesting Technical Support.

**Protected Data Disposal.** Boom Learning provides schools with deletion tools to manage data stores. Boom Learning periodically conduct deletion sweeps of stale Protected Data from unused teacher accounts.

**Subcontractor Oversight Details.** Boom Learning uses subcontractors. The current list is available at https://wow.boomlearning.com/blog/privacy. Boom Learning maintains agreements consistent with New York state, federal, and Education Entity legal requirements over the life of the contract. Educators will be given notice if any contract cannot be maintained consistent with this notice and an opportunity to cease use of the product. Subcontractors are under agreements that agree to maintain all data confidentially and to not to use our customers data for their purposes. Subcontractor agreements and relationships are reviewed annually. Subcontractor security practices are audited annually.

**Training.** All Covered Persons are trained annually. Training is conducted more frequently as a response to evolving threats within the education community. Boom Learning provides Boom Learning users with information bulletins about how to maintain the security of Protected Data. Users who opt our of our newletters will not receive such bulletins.

**Encryption.** Data is encrypted in transit and at rest using methods specified under Education Law 2-d 5(f)(5).

**Security Practices.** In addition to encryption in transit and at rest, Boom Learning uses the following measures and best practices to maintain the security and integrity of Protected Data.

- **a.** All Protected Data is stored behind authorization and authentication access points in cloud-storage on AWS cloud servers.
- **b.** Educators have access to student Protected Data. Parent or student requests for access to student Protected Data are referred to the Educator.
- **c.** Educators may use the "Private" setting for classrooms to suppress the visibility of Directory Information to students and parents.
- **d.** Passwords are encrypted in transit and at rest.
- **e.** Mobile app data is not persisted locally.
- **f.** All adult users have the ability to remotely log out all devices logged into an account in the event of a lost, missing or stolen device.
- **g.** Boom Learning limits access to Protected Data to Covered Persons with a need to know.
- **h.** Administrative rights are tailored to business needs with privacy and security considerations taken into account.
- **i.** The primary data store is protected with Two-Factor Authentication. Access is granted based on a neeed to know.
- **j.** Database downloads are on an as needed basis only, to a single machine, in a secured locked location behind a firewall. Downloads are deleted upon completion of the task requiring a download. The download machine is encrypted.
- **k.** The Boom Learning Chief Technology Officer shall enforce privacy by design and ensure testing, monitoring, and remediation of security systems. Boom Learning uses data minimization and privacy by design to minimize risk to Protected Data.
- **l.** Boom Learning performs continuous data backups. Backups are encrypted.

**Security Incidents.** The Privacy Legal Officer shall provide notice to the Educator of a security incident caused by a Covered Person that is determined to be a breach of Protected Data in accord with applicable statutory and regulatory deadlines. Upon learning of such incident, Educator shall promptly inform Boom Learning of any security incident, including those caused by the Educator, that is determined to be a breach of Protected Data**.**