Center for Technology

Data Privacy and Technology Integration Survey

The Moore Public Schools (MPS) Center for Technology Data Privacy and Technology Integration Survey was adapted from the Consortium for School Networking (CoSN) Privacy Toolkit to ensure potential MPS partners understand their duty and responsibility as well as the expectation of MPS regarding cybersecurity, data privacy, and the Family Educational Rights Privacy Act (FERPA) regarding the storage and management of student data. MPS also follows guidance from the Department of Education Student Data Privacy and from Access for Learning Community.

MPS strives to "Create Connections" for our students and staff – ensuring safe, efficient, and effective operations and communication is central to this process.

Completion of this survey does NOT guarantee a contract with the vendor or service provider.
Please complete this document and email to MPS contact that sent you the survey.

Current as of 11May2022

DATA PRIVACY AND TECHNOLOGY INTEGRATION SURVEY

--To be completed by potential MPS partner--

Potential Partner Company Name: Omega Labs Inc. dba Boom Learning
Completed Date: December 14, 2022
Name of Person Completing: Mary Oemig
Phone of Person Completing: 1-833-WOW-BOOM
Email of Person Completing: legal@boomlearning.com

I affirm that all information below is accurate and true as to our company's data privacy and integration practices.

Account Representative Name and Signature: _____
Mary Oemig, CEO

--If you ONLY provide links to your website and do NOT complete the information requested will be returned and may result in your exclusion for consideration—

Data Collection

Do you **AND** your associated 3rd Parties comply with all federal and state requirements like FERPA, COPPA, etc as defined by Protecting Student Privacy | U.S. Department of Education for any and all functions, such as analytics or PII?

Yes. We disclose our subprocessors in this list, which is updated annually.

Do you **AND** your associated 3rd Parties COMPLY with the General Data Protection Regulation (GDPR)? GDPR became enforceable on May 25, 2018. **Please provide a direct link to your public GDPR policy.**

Yes. We have been in compliance since 2018 and are members of the Privacy Shield and successor regimes. See our Privacy Notice for Data Exporters of Data About Non-US Data Subjects. We apply GDPR standards to all customers, regardless of location unless a more restrictive regime applies.

If you **AND/OR** the 3rd party does NOT meet above standards, do you assume risk and all associated costs such as mitigating data breach, credit history checks, etc?

We meet the above standards. The above standards require us to assume the risk and associated costs with mitigating risks caused by us or our third parties.

--If applicable and any of the above answers are "NO", this potential provider does NOT comply with federal guidance/policy and is a risk to MPS student/staff data. —

Data Security and Portability

Do you guarantee data portability in a usable format of all data elements collected and stored for MPS? What format will you provide this data back to MPS?

We provide MPS self-help tools to export and delete student data. Performance data is exportable in .csv format. If the DOE fails to delete data, we do per the deletion terms in https://wow.boomlearning.com/privacy to ensure stale data is not at risk. Deletions are unrecoverable.

Do you (including all associated 3rd parties) guarantee all data will be deleted with certification upon completion of a contract within 60 days?

We provided self-help data deletion. Data is deleted immediately on request. The data will be purged from offsite backups within 60 days. We certify in advance that if self-help tools are used data is purged within 60 days. If your team is unable to use self-help for any reason, customer service can process deletion for your account and provide a certification if requested.

Have you experienced any internal or external data breach or cybersecurity event within the last 24 months? If so, what was the issue and please explain action taken to communicate and resolve. ***A non-disclosure can be signed as needed.***

We had a data leak due to poor design by a partner OAuth (failure to use globally unique student identifiers). In rare cases, where two school districts both used the OAuth partner, and there was a student identifier used for both districts that was identical, a teacher at one district might see student performance data for a student at another school. We informed the OAuth partner, blocked the OAuth option until the leak could be patched, and worked with the OAuth partner to get it corrected. In an abundance of caution, we informed customers as soon as we were aware of the issue. We have occasional misdirected emails or account sharing by our customers. We inform them of the issue, make a log record if there was any risk of PII sharing, and provide support in mitigation, such as password resets. Our employees receive regular training on security and privacy. Failure to identify and escalate a data leak is a terminatable offense.

Will any data be stored outside the United States? Where is it stored?

All student PII data is all stored within the United States on AWS. Data is held in an AWS zone on the east coast. Our contract management provider is based in Denmark. Our contracts are stored there. The only PII in a contract would be the name and contact information of the school and signatory, along with the signature. Our Contracts provider is GDPR compliant and is planning to offer a US server.

How is your data at rest encrypted and protected (e.g. just passwords, passwords and sensitive data, all data)?

All data is encrypted at rest. User passwords, where they exist, are stored as a hash. Encryption meets HIPAA standards.

If the application is multi-tenant (several districts on one server/instance) hosting, how is data and access separated from other customers in the event of a data breach or event?

The application is multi-tenant. Data are stored encrypted and access is granted by role and by least privilege. No student data can be accessed without authentication.

How does the provider protect data in transit (e.g. SSL, hashing)?

All traffic uses SSL 1.2 and above.

Does the provider perform background checks on personnel with administrative access to servers, customer data? **You may be required to complete a "Declaration by Vendor" certifying your company has completed a sex offender verification on any employee with access to our student's records or access to our facilities.**

Yes. The only student information our employees can see are associated teachers and therapists, nickname, username, and performance reports. If an OAUTH provider delivers an avatar and email address we also have that. Employees do not have access to student addresses, phone numbers, parent information, or other sensitive information. Passwords are encrypted. Employees are subject to criminal records searches using Checkr (previously Good Hire).

Does the provider perform regular risk assessments, penetration testing, vulnerability management, and intrusion prevention?

All code is reviewed by at least two developers before it is deployed to look for vulnerabilities and potential security risks. We are under contract with a company to perform penetration/vulnerable scans. This test is currently being performed and will be repeated regularly.

Are backups performed and tested regularly and stored off-site?

Backups are performed, maintained, validated, and tested by our service provider which is hosted on AWS.

Will you provide certification of data destruction upon completion of contract? MPS requires all data to be provided back to MPS and associated data destroyed on your servers and/or third parties within 60 days of termination of contract.

We provided self-help data deletion. Data is deleted immediately on request. The data will be purged from offsite backups within 60 days. We certify in advance that if self-help tools are used data is purged within 60 days. If your team is unable to use self-help for any reason, customer service can process deletion for your account and provide a certification if requested.

Instructional Technology (IF APPLICABLE)

Have you signed the K-12 School Service Provider Pledge to Safeguard Student Privacy 2020? Are you willing to comply and sign the privacy pledge? Take The Pledge - Student Privacy Pledge | Pledge to Parents & Students

Boom Learning has signed the 2020 Student Privacy Pledge. https://wwow.boomlearning.com/privacy. Boom Learning had signed the prior Privacy Pledge also.

Do you **AND** your associated 3rd Parties ensure compliance with federal requirements under the Children's Internet Protection Act (CIPA) defined by the FCC's Children's Internet Protection Act (CIPA) | Federal Communications Commission (fcc.gov). **Failure to maintain CIPA compliance my result in immediate termination of contract and repayment back to the district.**

Yes. We are directed to adults: teachers and parents. Students cannot open accounts individually. Adults must create student accounts. We further assume all students are children, regardless of age and send the required notification to the adult who created the student account. Adults can "share" performance data about students. Doing so requires knowing the username of the second adult.

We ensure that each subprocessor with whom we share Student Data and/or Teacher or Principal Data are contractually bound by a written agreement that are engaged under a contract under which they agree that they have no right of access to our data stored in the subprocessors' cloud-based services.

Have you been vetted by another state educational entity that is part of the Access for Learning Community or state educational privacy alliance that is part of the COSN network. If so, please identify the state.

We are members of Access for Learning and the student Data Privacy Consortium and participate in consortium agreements and have for several years. We have 561 agreements through the consortium (see here and here). We have passed security review for New York City Schools. We have an agreement with the State of Tennessee. We are New York State Section 2d compliant.

Center for Technology

Data Privacy and Technology Integration Survey

Do you offer Single Sign On (SSO) or Rostering for teacher and/or student accounts? If so, can you work with our current solution(s) with OneRoster, Clever, Kimono, and GG4L **without** modifications or "work-arounds"? Is there an added cost?"

We offer SSO via Clever and the importing rosters from Clever at no extra cost. To access rostering from Clever, Boom Cards needs to be installed via an instructor's library and not at the district level.

Does your platform fully integrate with Canvas, Clever, Infinite Campus? Do you charge for these integrations?

We offer SSO via Clever and the importing rosters. We have a Canvas integration that is currently in beta testing. There is no extra charge to use these integrations.

(If applicable) Does your application allow for grade pass back to Infinite Campus and/or Canvas?

Our application does grade pass back into Canvas.

Does this program have embedded videos through Youtube, Vimeo, or other streaming sources?

The program itself does not contain any embedded videos. Some content, created for personal use, can contain videos from vimeo, youtube, and screencast-o-matic. Some content can be optionally acquired that contains Vimeo videos. The videos are not on a specific "channel." We take steps to prevent display of advertisements delivered by YouTube. Nonetheless, because YouTube reserves the right to deliver ads to children, we encourage teachers to prescreen video and use "Hide Card" to suppress any video that does not meet their school standards.

URLs that may be accessed by optional content:

- boomlearning.com
- vimeo.com
- youtube-nocookie.com
- screencast-o-matic.com

Does your instructional platform have stand-alone iOS and Android apps as opposed to accessing via web platform?

Yes.

To be completed by MPS Staff:

__ Y / __ N – Did the company provide the data checklist (Spreadsheet)

__ Y / __ N - Does the company adhere to federal/state/district data privacy regulations/guidance?

__ Y / __ N – Does the company integrate with MPS's current systems?

__ Y / __ N – Does the company meet the minimum requirements for their data security and implementation?

Reviewed by: _____ Date: _____