

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.

Current as of 19th Jan 2023

--To be completed by potential MPS partner--

Potential Partner Company Name: 3P Learning Inc

Completed Date: 19th Jan 2023

Name of Person Completing: Ravi Berry

Email of Person Completing: ravi.berry@3plearning.com

As the account representative, you affirm that all information below is accurate and true as to our company’s data privacy and integration practices. Failure to provide accurate information may result in termination of contract and return of payment to the district.

Account Representative Name: Ravi Berry



Signature:

--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 Privacy Standards

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 all functions?

Yes / No	Comment
Yes	More info here https://www.3plearning.com/privacy

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 / No	Comment
Yes	More info here https://www.3plearning.com/privacy

Are you **AND** your associated 3rd Parties in compliance with the [American Data Privacy and Protection Act \(6/21/2022\)](#)? If not, estimated time of compliance. **Please provide a direct link to your public policy if established.**

Yes / No	Comment
No	Within next 12 months

Are you **AND** your associated 3rd Parties willing to self-certify with the [Privacy Shield Framework](#)?

Yes / No	Comment
No	We already follow many standards across the globe and adhere to best practices with data and , privacy and security

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?

Yes / No	Comment
Yes	We take extreme precautions with data and aim to hold as little data as possible so that we can provide our services. We also have cyber insurances available in any unlikely event.

--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

Please check with Cybersecurity Framework(s) you and your 3rd party utilize in your ecosystem. **Please visit <http://www.edspex.org> for further details about the noted frameworks.**

Check those that Apply	MAINTAINING ORGANIZATION/GROUP	FRAMEWORK(S)
Yes	National Institute of Standards and Technology	NIST Cybersecurity Framework Version 1.1
	National Institute of Standards and Technology	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
	International Standards Organization	Information technology — Security techniques — Information security management systems (ISO 27000 series)
	Secure Controls Framework Council, LLC	Security Controls Framework (SCF)
	Center for Internet Security	CIS Critical Security Controls (CSC, CIS Top 20)
	Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S))	Cybersecurity Maturity Model Certification (CMMC, ~FAR/DFAR)
	OTHER: Cyber Essentials	Please explain: https://www.ncsc.gov.uk/cyberessentials/overview

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

Yes / No	Comment
----------	---------

Yes	Our main live data is stored in Amazon AWS Oregon USA. Backups are kept in Amazon Australia
-----	---

How is our data at transit and at rest be encrypted and protected?

Yes / No	Comment
Yes	Minimum AES 128bit+ encryption both in-transit and at rest

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?

Does the provider perform regular risk assessments, penetration testing, vulnerability management, and intrusion prevention? Please provide a date of last assessment.

Yes / No	Comment
Yes	We have regular 3 rd party independent penetration testing, we also have ongoing risk assessments and intrusion prevention activities. We also have a risk team who report directly to the board monthly.

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

Yes / No	Comment
Yes	Backups are taken nightly and stored offsite. We also have replication services in different data centers

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.**

Yes / No	Comment
No	No reportable breaches have occurred

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?

Yes / No	Comment
Yes	CSV or XLSX format

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

Yes / No	Comment
Partial	Request for data deletion MUST be sent to dpo@3plearning.com via an authorized rep from school or district. All data deletion is completed by an irreversible anonymization process.

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 / No	Comment
Yes	For specific staff in USA with direct access

Will you and your 3rd parties 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.**

Yes / No	Comment
Partial	Request for data deletion MUST be sent to dpo@3plearning.com via an authorized rep from school or district. All data deletion is completed by an irreversible anonymization process.

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](#)

Yes / No	Comment
Yes	We are willing to sign the pledge as we already adhere to responsible collection and use of student data

Do you **AND** your associated 3rd Parties ensure **all content and links within your application** is in 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 / No	Comment
Yes	

Do you have a National Data Privacy Agreement with 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 or district.

Yes / No	Comment
Unsure	We do have NDPA's with many other states in USA

Does your solution support accessibility and inclusivity (BEYOND W3C) for users by following the [accessibility criteria listed in ETSI EN 301 549](#)? Example: [Digital Learning Tools, Immersive Reader | Microsoft Education](#). If so, please explain or link to public web link as example. If not, what is the current roadmap to implement?

Yes / No	Comment
No	

Do you have a Single Sign On (SSO) or Rostering for teacher and/or student accounts? If so, can you work with our current solution(s) with Azure, Clever, GG4L **without** modifications or "work-arounds"?

Yes / No	Comment
Yes	With clever.com only

Does your platform fully integrate with Canvas or Clever?

Yes / No	Comment
Yes	Clever

Are there added cost for rostering, SSO creation, or any other integration needs?

Yes / No	Comment
No	

Does your application allow for preferred names versus legal names?

Yes / No	Comment
Yes	

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

Yes / No	Comment
No	

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

- Are the videos under a specific channel for ease of whitelisting settings?

- Provide example URL
- Vimeo
- Youtube
- Other: Please identify.

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

Yes / No	Comment
No	

To be completed by MPS Staff:

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?

NOTES:

Reviewed by: _____ Date: _____

Final Step: Upon Data Privacy and Integration approval, vendor will need to complete the OK_NDPA.