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: Scirra Limited
Completed Date: November 3rd, 2022
Name of Person Completing: Roger Henderson
Phone of Person Completing: +44 208 123 9369
Email of Person Completing: roger@construct.net

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: Roger Henderson 

--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**

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.**
https://www.construct.net/en/privacy-policy

If the 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

--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. —

Center for Technology

Data Privacy and Technology Integration Survey

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**?**

If the teacher assigns licenses using Access Codes (which is the recommended method of use) then <u>we do not acquire or store any personal information</u>. If licenses are assigned to a student personal account then we will store the student email address.

There is an option for students to submit work to a teacher. In the case a copy of the student game file is stored on a Microsoft Azure server for 72 hours and then automatically deleted. Scirra does not access these files.

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

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.*** **NO**

Will any data be stored outside the United States? Where is it stored? **NO. All data is stored on Microsoft Azure servers resident in USA**

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

Data at rest is encrypted. Passwords are not encrypted in the database, but are hashed using strong BCrypt hashing algorithm.

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?

Account access is by password protection.

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

All data is transmitted over HTTPS using TLS v.13, falling back to older versions of TLS where v.13 is not available.

.

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.

If the teacher assigns licenses using Access Codes (which is the recommended method of use) then <u>we do not acquire or store any personal information</u>. If licenses are assigned to a student personal account then we will store the student email address. We do not carry out UK sex offender verifications on employees.

Does the provider perform regular risk assessments, penetration testing, vulnerability management, and intrusion prevention? **No**

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

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. YES

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. That has just been completed

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

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.
No

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 provide single sign on through Google or Facebook.**

Does your platform fully integrate with Canvas, Clever, Infinite Campus? Do you charge for these integrations? **No**

(If applicable) Does your application allow for grade pass back to Infinite Campus and/or Canvas? **No. There is no such information stored in our system**

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.

No

Does your instructional platform have stand-alone iOS and Android apps as opposed to accessing via web platform?
No.

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: _____