

## Bill of Rights for Data Security and Privacy

The District is committed to protecting the privacy and security of student data and teacher and principal data. In accordance with New York Education Law Section 2-d and its implementing regulations, the District informs the school community of the following:

Parents and eligible students<sup>1</sup> can expect the following:

1. A student's personally identifiable (PII)<sup>2</sup> information cannot be sold or released for any commercial purposes.
2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency.
3. State and federal laws,<sup>3</sup> such as NYS Education Law §2-d and the Family Educational Rights and Privacy Act, that protect the confidentiality of personally identifiable information PII, 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 NYSED is available for public review at [www.nysed.gov/data-privacy-security](http://www.nysed.gov/data-privacy-security), and by writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234.
5. The right to have complaints about possible breaches and unauthorized disclosures of student data addressed.

○ Contact the District Data Protection Officer (or equivalent): Betsy Hardy,  
by email at [ehardy@fillmorecsd.org](mailto:ehardy@fillmorecsd.org) and/or phone at: 585-567-2251.  
More information may be found on the District website.

○ Complaints may also be submitted to NYSED online at [www.nysed.gov/data-privacy-security](http://www.nysed.gov/data-privacy-security), by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234, by email to [privacy@nysed.gov](mailto:privacy@nysed.gov), or by telephone at 518-474-0937.

<sup>1</sup> "Parent" means a parent, legal guardian, or person in parental relation to a student. These rights may not apply to parents of eligible students defined as a student eighteen years or older. "Eligible Student" means a student 18 years and older.

<sup>2</sup> "Personally identifiable information," as applied to student data, means personally identifiable information as defined in section 99.3 of title thirty-four of the code of federal regulations implementing the family educational rights and privacy act, section twelve hundred thirty-two-g of title twenty of the United States code, and, as applied to teacher or principal data, means "personally identifying information" as such term is used in subdivision ten of section three thousand twelve-c of this

chapter.

<sup>3</sup> Information about other state and federal laws that protect student data such as the Children's Online Privacy Protection Act, the Protection of Pupil Rights Amendment, and NY's Personal Privacy Protection Law can be found at <http://www.nysed.gov/student-data-privacy/federal-laws-protect-student-data>

6. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of their student's PII occurs.
7. Educational agency workers that handle PII will receive training on applicable state and federal laws, the educational agency's policies, and safeguards associated with industry standards and best practices that protect PII.
8. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

**BY THE VENDOR:**

Name: **Connor Pierson**

Contact Address: **privacy@quizizz.com**

Title: **Head of Marketing**



8/24/20

**Date**

## **EXHIBIT A (Continued)**

### **Supplemental Information about a Master Agreement between District and Quizizz Inc.**

District has entered into a Master Agreement with Quizizz Inc, which governs the availability to the District of the following products or services: Quizizz software, and/or apps, and/or technology tools, and/or web-services

Pursuant to the Master Agreement (which includes a Data Sharing and Confidentiality Agreement), the District may provide to Vendor, and Vendor will receive, personally identifiable information about students and/or teachers and principals that is protected by Section 2-d of the New York Education Law ("Protected Data").

**Exclusive Purposes for which Protected Data will be Used:** The exclusive purpose for which Vendor is receiving Protected Data from the District is to provide the District with the functionality of the products or services listed above. Vendor will not use the Protected Data for any other purposes not explicitly authorized above or within the Master Agreement.

**Oversight of Subcontractors:** In the event that Vendor engages subcontractors or other authorized persons or entities to perform one or more of its obligations under the Master Agreement (including subcontracting hosting of the Protected Data to a hosting service provider), it will require those subcontractors or other authorized persons or entities to whom it will disclose the Protected Data to execute legally binding agreements acknowledging their obligation under Section 2-d of the New York Education Law to comply with all applicable data protection, privacy and security requirements required of Vendor under the Master Agreement and applicable state and federal law and regulations.

### **Duration of Agreement and Protected Data Upon Termination or Expiration:**

- The Master Agreement commences on 7/1/2020 and expires on the end of use.
- Upon expiration of the Master Agreement without renewal, or upon termination of the Master Agreement prior to its expiration, Vendor will securely delete or otherwise destroy any and all Protected Data remaining in the possession of Vendor or any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data. If requested by the District, Vendor will assist the District in exporting all Protected Data previously received back to the District for its own use, prior to deletion,

in such formats as may be requested by the District.

- In the event the Master Agreement is assigned to a successor Vendor (to the extent authorized by the Master Agreement), the Vendor will cooperate with the District as necessary to transition Protected Data to the successor Vendor prior to deletion.
- Neither Vendor nor any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data will retain any Protected Data, copies, summaries or extracts of the Protected Data, or any de-identified Protected Data, on any storage medium whatsoever. Upon request, Vendor and/or its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data, as applicable, will provide the District with a certification from an appropriate officer that these requirements have been satisfied in full.

**Challenging Accuracy of Protected Data:** Parents or eligible students can challenge the accuracy of any Protected Data provided by the District to Vendor, by contacting the District regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or principals may request to challenge the accuracy of APPR data provided to Vendor by following the appeal process in the District's applicable APPR Plan.

**Data Storage and Security Protections:** Any Protected Data that Vendor receives will be stored on systems maintained by Vendor, or by a subcontractor under the direct control of Vendor, in a secure data center facility located within the United States. The measures that Vendor (and, if applicable, its subcontractors) will take to protect Protected Data include adoption of technologies, safeguards and practices that align with the NIST Cybersecurity Framework, and safeguards associated with industry standards and best practices including, but not limited to, disk encryption, file encryption, firewalls, and password protection.

**Encryption of Protected Data:** Vendor (and, if applicable, its subcontractors) will protect Protected Data in its custody from unauthorized disclosure while in motion or at rest, using a technology or methodology that complies with Section 2-d of the New York Education Law.