Parents Bill of Rights Relating to Student Data

The District, in compliance with Education Law 2-d, provides the following:

DEFINITIONS:
As used in this policy, the following terms are defined:

Student Data means personal identifiable information from the student records of a District student.

Teacher or Principal Data means personally identifiable information from District records 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.

Third-Party Contractor means any person or entity, other than a District, that receives student data or teacher or Principal data from the District pursuant to a contract or other written agreement for purposes of providing services to the District, including, but not limited to, data management or storage services, conducting studies for or on behalf of the District, or audit or evaluation of publicly funded programs. Such term shall include an educational partnership organization that receives student or teacher or Principal data from a school district to carry out its responsibilities pursuant to Education Law §211-e and is not a District, and a not-for-profit corporation or other nonprofit organization other than a District.

1. Neither student data, nor teacher or Principal data will not be sold or released for any commercial purpose;

2. Parents have the right to inspect and review the complete contents of their child's education record. Procedures for reviewing student records can be found in the Board Policy entitled: **#26 Policies and Procedures and Family Educational Rights and Privacy Act (FERPA) Notice for Directory Information** – *Section 1 – Legally Mandated Policies*;

3. Security protocols regarding confidentiality of personally identifiable information are currently in place and the safeguards necessary to protect the confidentiality of student data are maintained at industry standards and best practices. The safeguards include, but are not limited to encryption, firewalls, and password protection. As required by Education Law §2-d(5), the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (NIST Cybersecurity Framework or NIST CSF) is adopted as the standard for data security and privacy;

4. New York State maintains a complctc list of all student data collected by the State and the data is available for public review at http://www.p12.nysed.gov/irs/sirs/NYSEDDataElements2018.xlsx or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, NY 12234;

5. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to Records Access Officer, Joseph Gugino, Oxford Academy and Central School District, PO Box 192, Oxford, NY 13830;

6. The District will promptly acknowledge receipt of complaints, commence an investigation, and take the necessary precautions to protect personally identifiable information;

- Following its investigation of a submitted complaint, the District shall provide the parent or eligible student with its findings within a reasonable period but no more than 60 calendar days from receipt of the complaint;

- Where the District requires additional time, or where the response may compromise security or impede a law enforcement investigation, the District hall provide the parent or eligible student with a written explanation that includes the approximate date when the District anticipates that it will respond to the complaint;

- The District will require complaints to be submitted in writing;

- The District will maintain a record of all complaints of breaches or unauthorized releases of student data and their disposition in accordance with applicable data retention policies, including the Records Retention and Disposition Schedule ED-1;

7. This policy will be regularly updated with supplemental information for each contract the District enters into with a third-party contractor where the third-party contractor receives student data or teacher or Principal data. The supplemental information must be developed by the District and include the following information:

- The exclusive purposes for which the student data or teacher or Principal data will be used by the third-party contractor, as defined in the contract;

- How the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or Principal data, if any, will abide by all applicable data protection and security requirements, including, but not limited to, those outlined in applicable State and federal laws and regulations (e.g., FERPA; Education Law §2-d);

- The duration of the contract, including the contract's expiration date and a description of what will happen to the student data or teacher or Principal data upon expiration of the contract or other written agreement (e.g., whether, when and in what format it will be returned to the District and whether, when and how the data will be destroyed);

- If an how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or Principal data that is collected;

- Where the student data or teacher or Principal data will be stored, it will be described in such a manner as to protect data security and the security protections taken to ensure that such data will be protected and data security and privacy risks mitigated; and how the data will be protected using encryption while in motion and at rest will be addressed.

8. This policy shall be published on the District's website. This policy shall also be included with every contract the District enters with a third party contractor where the third party contractor receives student data or teacher or Principal data.

Agreement and Signature

By signing below, you agree to the Terms and Conditions in this Rider:

Company Name Kahoot! AS Product Name Kahoot!

Printed Name Espen Thoresen Signature  Date 4/16-2020

Adopted 5/9/16

Amended 6/1/20

Data Privacy Rider for All Contracts Involving Protected Data Pursuant to New York State Education Law §2-C and §2-D

Oxford Academy and Central School and the Third-Party Contractor agree as follows:

1. Definitions:
    a. Protected Information means personally identifiable information of students from student education records as defined by FERPA, as well as teacher and Principal data regarding annual professional performance reviews made confidential under New York Education Law §3012-c and §3012-d;
    b. Personally Identifiable Information (PII) means the same as defined by the regulations implementing FERPA (20 USC §1232-g);

2. Confidentiality of all Protected Information shall be maintained in accordance with State and Federal Law and the Oxford Academy and Central School's Data Security and Privacy Policy;

3. The Parties agree that the Oxford Academy and Central School's Parents' Bill of Rights for Data Security and Privacy are incorporated as part of this agreement, and the Third-Party Contractor shall comply with its terms;

4. The Third-Party Contractor agrees to comply with New York State Education Law §2-d and its implementing regulations;

5. The Third-Party Contractor agrees that any officers or employees of the Third-Party Contractor, and its assignees who have access to Protected Information, have received or will receive training on Federal and State law governing confidentiality of such information prior to receiving access;

6. The Third-Party Contractor shall:
    a. limit internal access to education records to those individuals that are determined to have legitimate educational interests;
    b. not use the education records for any other purposes than those explicitly authorized in its contract or written agreement. Unauthorized use specifically includes, but is not limited to, selling or disclosing personally identifiable information for marketing or commercial purposes or permitting, facilitating, or disclosing such information to another Third-Party for marketing or commercial purposes;
    c. except for authorized representatives of the Third-Party Contractor to the extent they are carrying out the contract or written agreement, not disclose any personally identifiable information to any other party;
        i. without the prior written consent of the parent or eligible student; or
        ii. unless required by statute or court order and the party provides notice of the disclosure to the New York State Education Department, Board of Education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by statute or court order;
    d. maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in its custody;

e. use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the Secretary of the United States Department of Health and Human Services in guidance issued under Section 13402(H)(2) of Public Law §111-5;
f. adopt technology, safeguards and practices that align with the NIST Cybersecurity Framework;
g. impose all the terms of this rider in writing where the Third-Party Contractor engages a subcontractor or other party to perform any of its contractual obligations which provides access to Protected Information.

Agreement and Signature

By signing below, you agree to the Terms and Conditions in this Rider:

Company Name Kahoot! AS Product Name Kahoot!

Printed Name Espen Thoresen Signature  Date 11/26-2020

Vendor's Data Security and Privacy Plan

Purposes of processing
Kahoot will use the student and teacher data only for the exclusive purpose of providing the service, as defined in the agreement. Kahoot does not use students data for any other purposes than the provision of services to the school/teacher.

Compliance with law
Kahoot! ensure that its data handling and security policies at any time complies with relevant data protection and privacy law. Kahoot runs regular security audits, and maintain systems and policies in accordance with state-of-the-art and industry best standards. Kahoot enters into written contracts with all our sub-processors imposing the same level of security and data protection obligations that are undertaken by Kahoot

Data storage and Encryption
Customer and user data will be stored at Kahoot's sub-processors, located, as applicable, in Europe, Canada and the USA. Kahoot! only uses hosting services that are ISO270001 and/or SOC2 type 2 compliant. Data is encrypted in motion and at rest in accordance with industry best standards. For datastores, Kahoot uses a combination of full partition encryption based on LUKS and supplied provided full disk encryption (AES).

Data is encrypted in motion and at rest in accordance with industry best standards;

a) At rest: Customer data only resides in the production environment encrypted with industry best practices (currently AES-256 or similar).

b) In motion: all network communication uses TLS v1.2 or higher. Kahoot's SSL implementation is rated A+ on the Qualys SSL Labs' SSL Server test.

Challenging the accuracy of the data
Kahoot will assist the school in potential requests from parents or students to access and/or correct data, as prescribed by relevant law.

Administrative, operational and technical safeguards
Kahoot! has robust data security and controls in place to ensure data privacy and protection, including a data security policy. The measures implemented to protect personal data includes; continuous Pen-testing by external vendor, information encryption in motion and at rest, access controls, password protection and regular awareness and privacy training for employees. Access to personal data is provided on a need-to-know basis. Kahoot holds SOC2 type 1 certification, and ensure that its sub-processors are certified at ISO270001 and/or SOC 2 level or similar. Kahoot has adopted NIST Framework for Improving Critical Infrastructure Security.

Employee training
Kahoot is committed to ensure the reliability and security of employees any other person acting under its supervision. Access to personal data is provided on a need-to-know basis and all employees are subject to duty of confidentiality. Mandatory security, awareness and privacy training is provide annually, including training on information handling and sector-specific demands.

Subcontractors
Kahoot enters into written contracts with all our sub-processors imposing the same level of security and data protection obligations that are undertaken by Kahoot. All sub-processors hold the highest level of security and have current certifications for ISO27001, SOC2 type 2, or similar. A list of our sub-processors are available online.

Security incidents
In addition to its data processing records, privacy policy and security measures, Kahoot! operates a

security incident response plan and train staff in detecting and handling a security breach – including notification to affected parties.

Destruction/return of data (upon termination)
Upon termination of the agreement, all personal data will be deleted and destroyed unless otherwise agreed.