



Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

Vendor Statement of Compliance Data Privacy and Protection

This agreement is entered into between the Roseville City School District ("LEA" or "District") and Kahoot! ASA ("Service Provider") on 05/15/2023 ("Effective Date").

WHEREAS, the LEA and the Service Provider entered into an agreement for Educational Technology services;

WHEREAS, the LEA is a California public entity subject to all state and federal laws governing education, including but not limited to California Assembly Bill 1584 ("AB 1584"), the California Education Code, the Children's Online Privacy and Protection Act ("COPPA"), and the Family Educational Rights and Privacy Act ("FERPA");

WHEREAS, AB 1584 requires, in part, that any agreement entered into, renewed or amended after January 1, 2015, between a local education agency and a third-party service provider must include certain terms;

NOW, THEREFORE, the Parties agree as follows:

Section I: General - All Data

1. **PASSWORD SECURITY.** All passwords are considered secure. Vendors may not disseminate any passwords unless specifically directed by Educational or Technology Services management. Vendors will not provide information concerning Admin accounts (ROOT Admin, container Admin, local NT administrator or Domain administrator) or their equivalent to any persons. District personnel ONLY will disseminate this information. Vendors will never create "back door" or "generic" user accounts on any systems unless specifically directed to do so by LEA management.

Agree: Yes No

2. **SYSTEM SECURITY.** Unauthorized access to or modification of District systems including file servers, routers, switches, NDS and Internet services is prohibited. Any attempt to bypass or subvert any District security system, both hardware, and software is prohibited.

Agree: Yes No

3. **PRIVACY.** The vendor will adhere to all provisions of the Federal Family Educational Rights and Privacy Act (FERPA, 20 U.S.C. 123g), California Education Code and district policies regarding the protection and confidentiality of data. At all times, the vendor will consider all data collected in the course of their duties to be protected and confidential. Release of this data can only be authorized by Technology & Information Services management and state and federal law.

Agree: Yes No



Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

Section I: General - All Data (Continued)

- 4. **REUSE:** Vendors shall not copy, duplicate, sell, repackage or use for demonstration purposes any Roseville City School District data without the prior, written consent of Educational or Technology Services management.
Agree: Yes No

- 5. **TRANSPORT:** Vendor must provide a secure channel (S/FTP, HTTPS, SSH, VPN, etc) for the District to "push" data to the vendor and to extract data as required. Vendors will not have direct access to District systems and will not "pull" data at any time.
Agree: Yes No

- 6. **EXTERNAL SECURITY:** Vendor must attach to this document reasonable evidence that their system is secure from external hacking and attacks. Devices such as firewalls and technologies such as NAT are the minimum requirements. Active IDS or similar technology is preferred.
Agree: Yes No

- 7. **INTERNAL SECURITY:** Vendors must attach to this document reasonable evidence that their system is secure from internal hacking and attacks. Describe the interactions vendor personal (or their representatives) will have directly with District data. How is uploaded data from the District handled and processed? Who has access to this data? What happens to the data after the upload is complete? What security safeguards are in place to protected unauthorized access to District data? How are backup performed and who has access to and custody of the backup media? How long are backup maintained; what happens to the District data once the backup is "expired"? If any data is printed, what happens to these hard copy records?
Agree: Yes No

- 8. **DISTRICT ACCESS:** Vendor must provide a secure means (see Item 5 above) for the District to extract ALL data from the vendor system. This can either be an online extraction tool or a vendor-provided extract as needed by the District (not to exceed quarterly). Describe the means and format of the data (delimited, Excel, MDB, SQL Dump).
Agree: Yes No

- 9. **TERMINATION:** Upon termination of this agreement as provided herein, the vendor will permanently delete all customer data from their system as allowed by state and federal law. Vendor may be required to certify the destruction of LEA data within 90 days of contract termination.
Agree: Yes No



Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

Section II: AB1584 Compliance - Student Information Only

1. Vendor agrees that the Roseville City School District retains ownership and control of all student data.
Agree: Yes No
2. Vendor must attach to this document a description of how student-created content can be exported and/or transferred to a personal account.
Agree: Yes No
3. Vendor is prohibited from allowing third-parties access to student information beyond those purposes defined in the contract.
Agree: Yes No
4. Vendor must attach to this document a description of how parents, legal guardians and students can review and correct their personally identifiable information.
Agree: Yes No
5. Vendor will attach to this document evidence how student data is kept secure and confidential.
Agree: Yes No
6. Vendor will attach to this document a description of procedures for notifying affected parents, legal guardians or eligible students when there is an unauthorized disclosure of student records.
Agree: Yes No
7. Vendor certifies that student records will not be retained or available to a third party once the contract has expired or is canceled (See Page 2, Item 9).
Agree: Yes No
8. Vendor will attach to this document a description of how they and any third party affiliates comply with FERPA.
Agree: Yes No
9. Vendor and its agents or third parties are prohibited from using personally identifiable information from student records to target advertising to students
Agree: Yes No



Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

Section III: SB 1177 SOPIPA Compliance - Student Information Only

1. Vendors cannot target advertising on their website or any other website using information acquired from students.

Agree: Yes No

2. Vendors cannot create a profile for a student except for school purposes as defined in the executed contract.

Agree: Yes No

3. Vendors cannot sell student information.

Agree: Yes No

4. Vendors cannot disclose student information unless for legal, regulatory, judicial, safety or operational improvement reasons.

Agree: Yes No

5. Vendors must attach to this document evidence of how student information is protected through reasonable security procedures and practices.

Agree: Yes No

6. Vendors must delete district-controlled student information when requested by the District.

Agree: Yes No

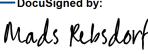
7. Vendors must disclose student information when required by law, for legitimate research purposes and for school purposes to educational agencies.

Agree: Yes No

As an authorized representative of my organization, I accept the conditions listed in this document.

Mads Rebsdorf

Print Name

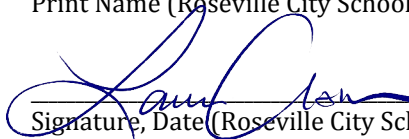


Signature, Date

1/5/2023 | 08:28 CEST

Laura Assem

Print Name (Roseville City School District)

 5/16/2023

Signature, Date (Roseville City School District)



Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

EXHIBITS

Section 1.6: External Security

Kahoot! is the world's leading game-based learning platform. Companies of all sizes use our platform to boost engagement and learning outcomes in everything from training and events to presentations and meetings. Organizations use Kahoot!'s best-in-class features to create a culture of continuous learning. Through interactive question types, collaboration tools, and powerful reports, L&D professionals are able to build an engaging, organization-wide learning experience that boosts training outcomes and simplifies knowledge sharing. What's more, thanks to enhanced user management tools, it's never been easier and more secure for IT admins to roll out Kahoot! across an organization.

Kahoot! uses end-to-end, industry-standard encryption in transit to end-users and internally between data centers and internal/external services. Data is always encrypted at rest.

We use multiple backup strategies for various parts of the platform. Backups are always encrypted and stored at a different site. Backups are kept for up to six months.

Our public certificates are obtained from an acknowledged certification authority, and we support TLS 1.2 or higher. What's more, the Kahoot! platform is SOC2 Type 2 compliant. We also run continuous penetration tests with an external party. A yearly report is available for enterprise customers.

You do not need to download anything to use Kahoot!, as it is a stand-alone website with no inbound connections. No installs, plugins, and integrations with internal systems are required to use Kahoot!. Optional integrations with Microsoft Teams and Zoom are available.

The Kahoot! platform is accessed from kahoot.com, while participants with no account can join games at kahoot.it. For an enhanced user experience, we recommend downloading the Kahoot! app on iOS or Android.

Kahoot! follows a number of policies to implement a safe and secure experience for users of all ages and to comply with relevant rules and regulations. Policies are reviewed on an annual basis to ensure they are kept up to date, and changes are approved by senior management.

Section 1.7: Internal Security

Kahoot! recognizes Customer information and data as the most critical aspect and important success factor in our business. Having our Customers trust in our handling of their data is crucial to drive Kahoot! forward as the leading learning platform vendor.

To ensure the data is secure we at Kahoot! have implemented a set of safeguards and processes covering all parts of the data journey. In addition, with new features and opportunities in our learning platform continuously being added, we are driven by clear policies, principles and procedures to ensure data stays secure.

Kahoot! have implemented and maintains the following security controls for customer and user data, consistent with globally cloud service provider industry best practices, including Controls, Policies & Procedures. Appropriate technical and administrative controls, and organizational policies and procedures.

Named person in the role as a dedicated Chief information security officer (CISO) with focus on security in all areas of the Kahoot! business.

Access Authorization. Access controls for provisioning users, which shall include providing Customers mechanism to view Customer users and their access privileges for licensed users.

Logging. System and application logging where technically possible. Kahoot! retains logs for a maximum one (1) month, verify such logs periodically for completeness.

Malicious code and/or software. Malware prevention software (e.g. antivirus) is implemented on infrastructure where applicable. Using Kahoot! does not demand any Customer hardware installment. Users can choose to install App on mobile devices.

System Security. System and IT security controls at Kahoot! follows industry best practices, including: (i) A high-level diagram, which will be provided to Customers upon request; (ii) Kahoot! use a mix of industry standard cloud and software firewalls to dynamically limit external and internal traffic between our services; (iii) A program for evaluating security patches and implementing patches using a formal change process within defined time limits; (iv) Kahoot! Runs continuous penetration testing by an independent third party, with a detailed written report issued annually by such third party and provided to Customers upon request; (v) Documentation of identified vulnerabilities ranked based on risk severity, and corrective action according to such rank.

Kahoot! runs regularly cross company Risk Assessments to ensure potential risks are identified and managed.

Kahoot! recognizes Customer information and data as the most critical aspect and important success factor in our business. Having our Customers trust in our handling of their data is crucial to drive Kahoot! forward as the leading learning platform vendor. Encryption. Kahoot! have implemented encryption on all Customer and user data.

Section II.2: Exporting of Student-Created Content

We allow customers to export their data, mainly provided in the JSON format. Please contact our Support team for more information.

Section II.4: Review and Correcting Personally Identifiable Information (PII)

Administrators may review and correct PII. If you use an email address provided by an Organization you are affiliated with (e.g. an employer or a school) to order the Kahoot! Service, you represent that you have authority to use that Organization's domain to sign up for a Service Plan in your capacity as a member of that Organization. The Organization, as the owner of the domain associated with your email address, may assume control over and manage your use of the Kahoot! Services. In such a case, your Organization's designated Administrator may (i) control and administer your account, including modifying and terminating your access and (ii) access and process your data, including the contents of your communications and files. Kahoot! may inform you that your associated Organization has assumed control of the Kahoot! Services covered by your Service Plan, but Kahoot! is under no obligation to provide such notice. If your Organization is administering your use of the Kahoot! Services or managing the tenant associated with your Service Plan, direct your data subject requests and privacy inquiries to your administrator. If your Organization is not administering your use of the Kahoot! Service or managing such tenants, direct your data subject requests and privacy inquiries to Kahoot! by contacting us at privacy@kahoot.com



Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

EXHIBITS

Section II.5: Securing Student Data

Our security measures include data encryption, firewalls, data use, and access limitations for our personnel and service providers, and physical access controls to our facilities. Our service providers that process payment data, maintain the applicable Payment Card Industry (PCI) compliance levels.

Section II.6: Disclosure Notification

N/A

You are responsible for maintaining the confidentiality of your account and any non-public authentication credentials associated with your use of the Kahoot! Services. You must promptly notify our customer support team about any possible misuse of your accounts, authentication credentials or any security incident related to the Kahoot! Services.

Section II.8: Family Educational Rights and Privacy Act (FERPA) Compliance

We comply with FERPA and COPPA when applicable to us. When FERPA applies, we act as a "school official" to our school or school district customer, which means that we are under the direct control of the school or district and use students' personal information only to provide our services to the school or district and not for our own purposes. To the extent COPPA applies, the school or district provides us with any necessary consent on behalf of students' parents or guardians to permit use of Kahoot! in the classroom.

Section III.5: How Student Data is Protected:

Kahoot! maintains a comprehensive security program designed to protect the security, privacy, confidentiality and integrity of Personal Information within our organization. We have in place appropriate and reasonable technical and organizational measures designed to protect Personal Information from loss, misuse, unauthorized access, disclosure, alteration, and destruction, taking into account the risks involved in the processing and the nature of the Personal Information. Our security measures include data encryption, firewalls, data use, and access limitations for our personnel and service providers, and physical access controls to our facilities. Our service providers that process payment data, maintain the applicable Payment Card Industry (PCI) compliance levels.

If you have any questions about the security of your Personal Information, you may contact us at privacy@kahoot.com.