KIDaccount Data Privacy and Security Policy

Introduction

At KIDaccount, we are committed to protecting your privacy. We take pride in keeping all school and student PII safe and private. KIDaccount evaluates our privacy practices and standards on a regular basis to increase data privacy. This Privacy Policy explains how we collect, use, and disclose PII in connection with KIDaccount Services.

KIDaccount provides safety and accountability software services to schools and other entities. KIDaccount, in its role as a vendor contracted to perform outsourced service to our Customers, shall access a limited amount of necessary personally identifiable information (PII) contained in student records to allow you to utilize the Hosted Software. These disclosures are authorized under the Family Educational Rights and Privacy Act (FERPA), a federal statute that regulates the privacy of student records by any school that receives financial assistance from the U.S. Department of Education. KIDaccount, as your contractor receives the disclosures on the same basis as school officials employed by you, consistent with the Family Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. § 1232g (34 CFR Part 99); the Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. § 6501-6506 (16 CFR Part 312) FERPA regulations. KIDaccount has a legitimate and necessary educational interest in the information to provide the Hosted Software. KIDaccount is directly controlled by the Customer, in using and maintaining the disclosed education records, in accordance with the terms of its contract.

KIDaccount acknowledges it is subject to the same conditions on use and redisclosure of education records that govern all school officials, as provided in 34 CFR §99.33. KIDaccount must ensure that only it's employees, contractors or those employed by its contractors, with a legitimate educational interest consistent with the purposes for which you obtained the information, may obtain access to PII maintained by KIDaccount on behalf of you. Further, in accordance with 34 CFR §99.33(a) and (b), KIDaccount may not redisclose PII without consent of a parent or an eligible student (meaning a student who is 18 years old or above or is enrolled in postsecondary education) unless you authorize the redisclosure under a FERPA exception and you record the subsequent disclosure.

This policy does not apply to PII that we collect through means other than our services such as through our marketing website www.kidaccount.com and other offline business practices unrelated to our services. Please refer to our Website Privacy Policy here: Privacy Policy - KIDaccount

Data Collected

1. **What data is collected**

   KIDaccount offers several services to our customers. Depending on the services we are providing, we may collect PII in a variety of ways. KIDaccount collects the following PII about any school staff member, student, visitor, or volunteer that enters a customer's building:

   - District: District Name, School Name(s), Start/End Date, Start/End Time

- Student: School ID, First Name, Last Name, Grade, Classroom or Class Schedule, Dismissal Method Information including Bus number, Special notes, Attendance, Events such as Afterschool programs, field trips, etc., Student Contacts (Parents, Legal Guardians, Emergency Contacts)
- Student Contacts (Approved and Banned): First Name, Last Name, Contact Status (Primary, Approved or Banned), Contact Relationship, Cell Number, Email, Contact Check In/Out Signature, Check In/Out Reason, Government Issued identification (e. g., driver's license, state ID, military ID), Photograph upon entering the building. Any other information our customers have requested to be collected from you on their behalf.

KIDaccount will comply with lawful requests by public authorities to disclose PII including to meet national security or law enforcement requirements. We may also share your PII as required by law in accordance with a court order, subpoena, or other legal process, or when we believe in good faith that disclosure is necessary to protect our rights, protect your safety, the safety of others, to investigate fraud, or to respond to a government request.

2. How Data is Collected

Data is provided to KIDaccount by our Customers either directly, by manual entry, or from their Student Information System (SIS) or other third-party systems integrating with the school's SIS.

3. Who owns the Data

KIDaccount understands and respects that you have put trust in KIDaccount and KIDaccount shall take all reasonable efforts to ensure student data, information, and privacy is always kept completely confidential and secure. KIDaccount is a hosting service and does not own or manage any of the student or district-created data. The data within the Hosted Software is the property of, and under the control of, the Customer.

4. Data Removal

KIDaccount does not and will not delete, change, or disclose any information from the Hosted Software without your consent or as required by law. Upon request from our Customers, we will return, delete, or destroy students, staff, visitor, volunteer and any other PII stored by us in accordance with applicable law and our Customer's requirements. Customers may request the deletion of data by emailing customerservice@kidaccount.com.

5. Data Retention

KIDaccount does not modify, correct, or delete the data of students, staff, visitors, volunteers, or other individuals without written instructions from our Customers to do so. We will retain student, school staff, visitor, volunteer, or any other PII for the duration of the agreement with

our Customers. Please contact customerservice@kidaccount.com for production or deletion of data.

Security

1. **How data is protected**
   KIDaccount is committed to ensuring that all PII entrusted to us is secure and protected. We limit the data collected to only required data to fulfill the needs of our Customers and is generally regarded as Directory Information. KIDaccount follows NIST Privacy Framework and NIST Cybersecurity Framework.

   KIDaccount performs initial security awareness as part of employee onboarding, then requires annual refresher. KIDaccount restricts physical system access to only authorized personnel. We monitor and log physical access to the information system and maintain access records. KIDaccount monitors and responds to physical intrusion alarms and surveillance equipment. All Datacenter PE related controls are the responsibility of Leveraged Service-Rackspace Technology. KIDaccount restricts access to authorized personnel at both the VPN and local host level.

   KIDaccount ensures secure separation of customer data. Each customer's data resides within a unique database.

2. **Data Encryption**

   KIDaccount ensures Data at Rest and OS Authentication modules are FIPS 140-2 Compliant. NSA approved algorithms are used for all encryption modules relating to block ciphers, digital signatures and hash functions. Cryptographic modules relating to Transmission and Remote Access are FIPS 140-2 Validated and NSA Approved. KIDaccount Webpage is TLS 1.2 Compliant. The Webpage and System Interconnections are TLS 1.3 Compliant.

   KIDaccount reviews monthly vulnerability reports and mitigates any critical vulnerabilities within 30 days. The current vulnerability report ran on 9/21/23 shows no critical vulnerabilities.

3. **Password**

   KIDaccount creates secure connections by integrating Google SSO into the user authentication process. The standard login process requires a minimum 12-character password.

4. **Multi-Factor Authentication**

   KIDaccount requires all employees with access to Customer data to use SSO with 2-Step authentication for login.

   KIDaccount recommends all customers using SSO login to also require a 2-Step authentication for login.

2-Step authentication is available for all customers using a standard login.

5. **Cookies**

Cookies Policy for Customer User Site:
KIDaccount only uses Session ID Cookies for login purposes on our customer site. These cookies are required, and the user cannot login to the website without these cookies. Session cookies last for a session and are stored in a temporary memory location. This temporary memory location and the cookies are deleted when you leave the website or close your browser. Session cookies are never stored on your device. Session cookies are GDRP compliant.

KIDaccount does not track analytics cookies on our customer's site.

Cookies Policy for Marketing Website:
KIDaccount's Privacy Policy for our marketing website can be found at www.kidaccount.com/privacy-policy. You can choose to refuse all cookies or to indicate when a cookie is being sent. However, if you do not accept cookies, you may not be able to use some portions of our service.

Third-Party Data Sharing

1. **Third-Party Services**
The use of all third-party services is strictly for application functionality and security.

#	External System Connection	Description	Information Shared
1	Text Alert System	System interconnection used to send SMS Alerts	Specified Staff Phone Numbers
2	SSO	System interconnection used for Single Sign On (SSO) authentication	Staff and Student Email
3	Sex Offense Screening	System interconnection used to perform Sex Offender Registry Search	Government Issued Identification (e. g., driver's license, state ID, military ID)
4	Student Information System (SIS) connections	System Interconnection used to import/export School Data	KIDaccount imports directory information from Student Information Systems. KIDaccount does not share data with Student Information Systems.

	Student Information System Connection Services	System Interconnection used to import/export School Data	KIDaccount imports directory information from Student Information System Connection Services. KIDaccount does not Share data with Student Information System Connection Services.

KIDaccount does not publicly disclose the names of third-party vendors for security purposes. Customers can request a list of 3rd Party Vendors by contacting KIDaccount at customerservice@kidaccount.com.

2. **Opt-Out Policy**

Customers can opt-out of third-party data sharing. This may affect the functionality of some aspects of the services provided. To opt out, please contact us at customerservice@kidaccount.com.

3. **Third-Party Privacy Practices**

Third-Party Vendors are required to adhere to the terms of the KIDaccount-Customer agreement.

4. **Notification of Change in Third-Party Services**

Customers will be notified of any change in Third-Party Services within 60 days of said changes. All new third-party vendors are required to adhere to the terms of the KIDaccount-Customer Agreement.

Advertising

No targeted or third-party ads are displayed on the KIDaccount customer platform. Third party services are not used for ads or tracking. KIDaccount only tracks interactions within its application and does not use any tracking technologies for ads.

KIDaccount will not sell or share student or Customer PII.

Contact Information

Contact KIDaccount with any questions about this policy or our privacy and security practices at customerservice@kidaccount.com.

Policy Updates

Data Privacy and Security is a high priority for KIDaccount and our Customers. We reserve the right to change or amend this Policy at any time to provide the most appropriate privacy and security for our customers. The latest revised Policy will be available to our customers on the KIDaccount Customer Help page.

Policy Revised September 21, 2023