Kid Account, LLC Privacy Policy

KIDaccount respects your student data use and privacy. We understand that you have put your trust in us to ensure that your information is kept confidential and secure. The purpose of this Privacy Policy is to inform you what personal information we may collect and how we use such information. As you know, our primary purpose in collecting information from you is so that you may use KIDaccount to assist you in the school dismissal process and other associated applications. We do not sell, rent or otherwise disclose your personally identifiable information, including name, address, e-mail address or contact information, to third parties.

KIDaccount, in its role as a vendor to educational agencies and institutions (EAs), receives disclosures from the EAs of personally identifiable information (PII) contained in student records. Only information that is needed for KIDaccount to perform services outsourced to it by the EA is disclosed to KIDaccount. These disclosures are authorized under the Family Educational Rights and Privacy Act (FERPA), a federal statute that regulates the privacy of student records by EAs that receive financial assistance from the U.S. Department of Education. KIDaccount, as a contractor to the EA, receives the disclosures on the same basis as school officials employed by the EA, consistent with FERPA regulations, 34 CFR §99.31(a)(1)(i)(B). Consistent with those regulations, KIDaccount has a legitimate educational interest in the information to which it is given access because the information is needed to perform the outsourced service, and KIDaccount is under the direct control of the EA in using and maintaining the disclosed education records, consistent with the terms of its contract.

KIDaccount 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. In particular, KIDaccount must ensure that only individuals that it employs or that are employed by its contractor, with legitimate educational interests – consistent with the purposes for which KIDaccount obtained the information -- obtain access to PII from education records it maintains on behalf of the district or institution. 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 the agency or institution has authorized the redisclosure under a FERPA exception and the agency or institution records the subsequent disclosure. An example of such a disclosure is when KIDaccount is requested by a school district to assist the district in the transfer of the student records from our system to another system.

KIDaccount gives EA access to provide the following data for the use in KIDaccount application:

DISTRICT
School Name, School District, Start/End date/time

STUDENT
ID First Name Last Name, Gender, Grade, Classroom, Travel Type, Status (In school, Absent, Dismissed, Disciplinary – ie ISS), Bus Route, Special Notes, Custom Dismissal Schedule, Events (After school, etc.)

PARENT
First Name, Last Name, Contact First Name, Contact Last Name, Contact Status (ie: primary, approved or banned), Relation Code, Contact Type, Comments, Cell Number, Email, Parent Check In/Out Signature, Check In/Out Reason

STAFF
First Name, Last Name, Email, Position

The collection, input, use, retention, disposal, and disclosure of any information in our software applications are controlled solely by the EAs which license our products and may include additional data as necessary by the EA requirements. KIDaccount will not sell education records for targeted advertising or marketing purposes. KIDaccount uses data within its products to deliver the services contracted by the educational institution. KIDaccount may use anonymized, non-PII data internally to improve the products and services it delivers to EAs.

KIDaccount takes protecting your student information seriously. Our servers are stored in secure, access controlled rooms and are located behind industry leading firewalls that are monitored and maintained by highly trained security professionals 24/7. In addition, The KIDaccount Website and Mobile App are protected by industry standard SSL encryption algorithms that are constantly evolving. This helps to insure that the connection between sensitive data and the end user is safe from preying eyes or third parties.

KIDaccount employs extensive technological and operational measures to ensure data security and privacy, including advanced security systems technology, physical access controls, and annual privacy training for employees, and criminal background checks of all employees. All data is housed within the United States. Details about the company policies which support the KIDaccount security programs are available to EAs under a non-disclosure agreement. Unfortunately, despite these security measures, no data transmission over the Internet can be guaranteed to be 100% secure. As a result, while we strive to protect your personal information, we cannot guarantee or warrant the security of any information you transmit to or from our website, and you do so at your own risk. Therefore, we cannot be and are not responsible for unauthorized access to your information that is the result of hackers or others who have obtained access through illegal measures, hardware or software failures, acts of God or any other factors that compromise the security of the data we collect.

Our failure resistant servers are built with redundant hardware including RAID hard drives to help minimize the possibility of a server failure. However, in the unlikely event that a server should fail, another server will automatically be activated to take its place. KIDaccount data is replicated to a backup server every hour, helping to not only insure 99.999% uptime, but also that your data is as up to date as possible

KIDaccount does not own any of the student data or district-created data within its products. These data within the products are property of, and under the control of the local educational agency. KIDaccount will not delete, change, or disclose any information from our software applications controlled by the EA without EA consent.

In the event any third party (including the eligible student or parent/guardian of the eligible student) seeks to access education records, KIDaccount will immediately inform the EA of such request in writing. KIDaccount shall not provide access to such data or information or respond to such requests unless compelled to do so by court order or lawfully issued subpoena from any court of competent jurisdiction or directed to do so by the EA. Should KIDaccount receive a court order or lawfully issued subpoena seeking the release of such data or information, KIDaccount shall provide immediate notification, along with a copy thereof, to the EA prior to releasing the requested data or information, unless such notification is prohibited by law or judicial and/or administrative order or subpoena.

If the EA is unable to fulfil a request of an eligible student or parent/guardian to review the student's records, KIDaccount can assist at the direction and expense of the EA. In such an event where a parent, legal guardian, or eligible student seeks to make changes to the data within our products parents, legal guardians, or eligible students shall follow the procedures established by the EA in accordance with FERPA. Generally these procedures establish the right to request an amendment of the student's education records that the parent or eligible student believes is inaccurate, misleading, or otherwise in violation of the student's privacy rights under FERPA. Parents or eligible students who wish to ask the EA to amend their child's or their education record should write an EA official (often a Principal or Superintendent), clearly identify the part of the record they want changed, and specify why it should be changed. If the EA decides not to amend the record as requested by the parent or eligible student, the EA will notify the parent or eligible student of the decision and of their right to a hearing regarding the request for amendment. Additional information regarding the hearing procedures would be provided to the parent or eligible student when notified of the right to a hearing.

In the event KIDaccount becomes aware of a data breach or inadvertent disclosure of PII, KIDaccount shall take immediate steps to limit and mitigate such security breach to the extent possible. A senior executive of KIDaccount will notify a senior member of the affected EAs leadership team, ideally the Superintendent or similar chief executive. This typically will occur within 24 hours of confirmation of the event and would include the known relevant details. The EA and KIDaccount will work cooperatively in determining an action plan, including any required notification of affected persons. In the event that KIDaccount is at fault for the breach or disclosure, KIDaccount carries a $1,000,000 liability insurance policy.

In the event of termination of a license to use our products, KIDaccount works with the EA, in accordance of the terms of the EAs contract, to destroy all student records contained in our systems and then will permanently delete all archival or backup copies of the agency's or institution's data. KIDaccount shall not knowingly retain copies of any data or information received from EA once EA has directed KIDaccount as to how such information shall be returned and/or destroyed. Furthermore, KIDaccount shall ensure that it disposes of any and all data or information received from EA in a commercially reasonable manner that maintains the confidentiality of the contents of such records (e.g. shredding paper records, erasing and reformatting hard drives, erasing and/or physically destroying any portable electronic devices). At the request of the EA, KIDaccount will provide a written certification of destruction.

To the extent parents, guardians or students have questions regarding the content of, or privacy associated with, any applications used by the educational institution, please contact that agency or institution.

KIDaccount may, from time to time, update this policy to be in compliance with evolving state and federal laws and regulations. We will not materially change our policies and practices to make them less protective of your privacy without the written consent of the EA and the EA may rely upon any and enforce any current or prior version of this policy unless otherwise agreed to in writing.

COPPA Compliance

The Children's Online Privacy Protection Act (COPPA) does not apply to KIDaccount. The KIDaccount Products do not collect personally identifiable information (PII) from children under the age of 13. PII collected and maintained within the KIDaccount products is entered by adults; either the child's parent or guardian during an enrollment process or by the school officials that use our products to operate the school. Access to the system is granted to all users by the educational agencies and institutions (EAs) which license our products.

Please note that the collection, input, use, retention, disposal, and disclosure of any private information in our software applications are controlled solely by the EAs which license our products. KIDaccount will not delete, change, or disclose any information from our software applications controlled by the EA without EA consent. To the extent parents, guardians or students have questions regarding the privacy associated with the applications provided by the EA, please contact that agency or institution.

HIPAA Compliance

Student records that are disclosed to KIDaccount by EAs and maintained within KIDaccount products are by definition "education records" under FERPA and not "protected health information" under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Because student health information in education records is protected by FERPA, the HIPAA Privacy Rule excludes such information from its coverage. See the exception at paragraph (2)(i) to the definition of "protected health information" in the HIPAA Privacy Rule at 45 CFR § 160.103. See, also, Joint Guidance on the Application of the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to Student Health Records, USED and U.S. Department of Health and Human Services (November 2008