



Kids Discover, LLC  
192 Lexington Avenue  
New York, NY 10016  
Phone: (212) 677-4457

April 15, 2020

## **Data Security and Privacy Plan: Kids Discover Online** Amended for New York State

### **Introduction**

The purpose of this document is to outline the various technologies, safeguards, and business practices that Kids Discover, LLC (Kids Discover, the Company) employs in order to appropriately handle and protect any and all student data or teacher or principal data the Company may receive in conjunction with the services it offers. When reading this document, it is important to note that Kids Discover Online, the digital platform the Company offers its services through, collects a minimal amount of Personally Identifiable Information (as defined below). In some instances, Kids Discover Online may not collect any Personally Identifiable Information in order to provide its full suite of services to School Districts and Educational Agencies, particularly when services are delivered to school library systems. Any questions, inquiries, or clarifications regarding this document should be directed to [questions@kidsdiscover.com](mailto:questions@kidsdiscover.com), and a Kids Discover Representative will reply in a timely manner.

### **Definitions**

1. As it pertains to this Data Security and Privacy Plan, in accordance with New York State Education Law 2-d, the following terms shall have the following meanings:
  - a. Breach means the unauthorized acquisition, access, use, or disclosure of student data and/or teacher or principal data by or to a person not authorized to acquire, access, use, or receive the student data and/or teacher or principal data
  - b. Commercial or Marketing Purpose means the sale of student data; or its use or disclosure for purposes of receiving remuneration, whether directly or indirectly; the use of student data for advertising purposes, or to develop, improve or market products or services to students.
  - c. Education Records means an education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.
  - d. Educational Agency means a school district, board of cooperative educational services (BOCES), school, or the Department.
  - e. Encryption means methods of rendering personally identifiable information unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified or permitted 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. Parent means a parent, legal guardian, or person in parental relation to a student.
  - g. Personally Identifiable Information, as applied to student data, means personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g, and as applied to teacher and principal data, means personally identifiable information as such term is defined in Education Law §3012-c (10).
  - h. School means any public elementary or secondary school including a charter school, universal pre-kindergarten program authorized pursuant to Education Law §3602-e, an approved provider of preschool special education, any other publicly funded pre-kindergarten program, a school serving children in a special act school district as defined in Education Law §4001, an approved private school for the education of students with disabilities, a State-supported school subject to the provisions of Article 85 of the Education Law, or a State-operated school subject to the provisions of Articles 87 or 88 of the Education Law.

- i. Student means any person attending or seeking to enroll in an educational agency.
- j. Student Data means personally identifiable information from the student records of an educational agency.
- k. Teacher or Principal Data means personally identifiable information from the records of an educational agency 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.

## **Data Security Framework and Protocols:**

### **Cybersecurity Risk Assessment and Management**

- Cybersecurity comes in all shapes and sizes. It is wholly dependent on the type and amount of data that is being collected, managed, stored, and utilized in order to deliver a particular service. Kids Discover Online offers an online library of science, social studies, and nonfiction reading for elementary and middle school aged students. In order to provide this service, Kids Discover Online requires a minimal amount of student data or teacher or principal data. In some instances, Kids Discover Online may not require the collection of any student data or teacher or principal data whatsoever.
  - Collecting a minimal amount of student data or teacher or principal data is the first step in mitigating cybersecurity risk.
  - This minimal amount of collected data also simplifies Kids Discover's management and protection of such data, and therefore informs the software, hardware, and overall systems in place to achieve strong, reliable cybersecurity.
  - It also informs the limited number of Kids Discover personnel that have (and need) access to such data at any given time, along with the extent of proper training that those individuals receive.

### **Data Collection and Protection**

- The Personally Identifiable Information that Kids Discover Online may collect is limited to the following student data or teacher or principal data:
  - Student Data PII
    - First Name and Last Name
      - NOTE: Kids Discover Online does not collect student email addresses, and explicitly prohibits the collection of Student PII other than First and Last Name. For example, NONE of the following examples of Student PII are collected:
        - Name of student's parent or other family members
        - The physical address of the student or student's family
        - A personal identifier, such as student's social security number or student number
        - Student's date of birth
        - Student's attendance
  - Teacher or Principal PII
    - First Name and Last Name
    - Email Address
    - Job Title or Role
    - School Building Name and Address, including Zip Code
      - Kids Discover Online explicitly prohibits the collection of any other personally identifiable information for any Teacher or Principal that uses the service.
- Student data or teacher or principal data that is collected by Kids Discover Online and used to provide the services are protected in the following ways:
  - Access to any and all student data or teacher or principal data is limited to authorized Kids Discover personnel, and requires Company issued credentials that are updated every 3 months. The number of Kids Discover personnel with authorization is limited to individuals that have received proper training, and fully understand their roles and responsibilities.

- All authorized personnel have received training from IT professionals and senior executives at Kids Discover.
- Authorized personnel in charge of the development, management, maintenance, and overall support of critical systems, software, and hardware that stores such data are IT professionals with graduate degrees and extensive training in IT and Cybersecurity Operations.
- Student data or teacher or principal data that is collected by Kids Discover Online is stored in a cloud managed, enterprise grade Microsoft Azure SQL Server Database. The database utilizes the SHA1 hashing algorithm, with a hash sequence of 160 bits in length.
  - Data is automatically backed up every 24 hours.
  - Database capacity is 250GB, more than double the capacity needed to effectively store and run its contents.
  - Kids Discover Online utilizes three different development environments, including a local environment, staged environment, and production environment for both the database and general code base of the platform. This ensures that any testing, enhancements, bug fixes, data handling and/or data conversions are executed in two different test environments before being executed in a production environment (with live data).
  - Data that has been dormant for 12 months is automatically deleted from the database.
    - Data can be deleted within 24 to 48 hours by written request from any School, School District, Educational Agency, or Customer.
    - Data can be provided and delivered to any School, School District, Educational Agency, or Customer within 24 to 48 hours by written request.
- Kids Discover Online's database is virtually managed. Updates and upgrades are performed through Kids Discover's Microsoft Azure account, utilizing Microsoft Azure's market leading infrastructure and resources.

### **Systems Monitoring and Detection**

- Kids Discover utilizes a suite of tools afforded by Microsoft Azure to monitor, detect, and in turn alert Kids Discover personnel of any anomalous activity.
  - Examples of anomalous activity may include, but are not limited to:
    - Traffic spikes from non-customer IP addresses
    - Service interruptions
    - Elevated levels of server errors
    - Brute force attacks
    - Microsoft-issued systems updates
  - Kids Discover personnel are alerted in real-time to anomalous activity based on predetermined thresholds and triggers. Depending on the nature of the anomalous activity and subsequent alert, Kids Discover personnel are clear in their roles and responsibilities in terms of response time and prioritization.

### **Response and Recovery**

- Once an anomaly is detected, authorized Kids Discover personnel will conduct an investigation that includes, but is not limited to:
  - Review and analysis of server logs
  - Review and analysis of database contents
  - System performance tests and security audits
- Information is then shared to the appropriate Kids Discover personnel, including Kids Discover Management, to determine the depth and magnitude of any further investigations and potential data recovery procedures needing to be conducted.
- If it is determined that an incident such as a data breach has occurred, and that any data may have been effectively altered or compromised from the resulting incident, Kids Discover personnel will

then notify any customers, Schools, or Educational Agencies as defined in this document of the nature of the incident, whose data may have been affected.

- It is important to note that Kids Discover views all customers as partners and will work diligently to communicate transparently to all stakeholders of any issues or incidents that have arisen.
  - Kids Discover will continue to communicate with any customers, Schools, or Educational Agencies until the issue has been resolved and rectified, and both parties agree about the best possible path forward.
- Kids Discover will then work to restore, retrieve, correct, and improve any and all affected data, along with the systems, software, hardware, and general processes that resulted in the situation.