Renaissance customers
Summer 2019

Data privacy and security overview

As a leading provider of technology and service to K–12 schools worldwide, security is a critical aspect of Renaissance's business. We strive to exceed the expectations of the educators we serve, as well as those of the laws, rules, and regulations created to keep data confidential. Every day, millions of users depend upon our commitment to ensure their information is kept safe and confidential. We take this commitment seriously. This document addresses common inquiries regarding Renaissance's data collection, data privacy, and data security.

Schools control and own data collected within their Renaissance sites

Each school or district owns its data, including personally identifiable information. The data owner is the only entity that may access and manage student-level data, including adding, editing, or deleting information about the educational group, its schools, school years, personnel, students, courses, and classes.

Renaissance limits the amount of personally identifiable information it collects. Table 1 identifies the data that is required, by role, for users to access Renaissance applications, as well as optional user information that schools may choose to provide. Optional student data points, such as students' ethnicities, demographic characteristics, and native language spoken, can provide teachers and administrators with a more detailed perspective of achievement and growth.

Table 1. Renaissance limits the personally identifiable user data it requires schools to provide.

User role	User data that is required to provide access to Renaissance solutions	Optional user data schools may provide, if desired
Student	• First name (one character minimum) • Last name (one character minimum) • Username (auto-generated by Renaissance unless entered by school or educational group) • Password • School enrollment • Local student ID (auto-generated by Renaissance unless entered by school or educational group) • Grade level • Date of birth • Assessment or practice data	• Preferred name • Middle name • Gender • State student ID • Ethnicity • Language • Demographic characteristics
Personnel	• First name (one character minimum) • Last name (one character minimum) • Username (auto-generated by Renaissance unless entered by school or educational group) • Password • School • Local ID (auto-generated by Renaissance unless entered by school or educational group)	• Salutation • Preferred first name • Middle name • State personnel ID • Primary position • Gender

Any data used for research is stripped of personally identifiable information. At no time will Renaissance publish the names of any district, school, or individual without written authorization. Renaissance collects select elements of metadata, which Renaissance's developers use to deliver the appropriate user experience based upon the way in which the user interacts with Renaissance's applications. The metadata collected is IP address, access data/time, referring URLs, page views, browser type, and device type and operating system.

Renaissance employs multiple measures to keep users' data secure

Renaissance solutions are password protected. Each school or district has a unique URL to access its Renaissance solutions. Each user is assigned unique login credentials, which must be authenticated before the user can access the school or district site. Users are assigned to distinct roles, such as student, teacher, or administrator, which limits what information users can access or edit.

myON Reader and myON News data is encrypted in transit and at rest. Data for applications hosted within the Renaissance Growth Platform environment is encrypted in transit and at rest. Data for applications hosted within the Renaissance Data Center environment is housed on a closed system. This means that the secure web-based servers, storage, and databases that support Renaissance solutions are dedicated only for that purpose. Each customer has its own segregated database. Renaissance is working to upgrade all United States customers to the Renaissance Growth Platform hosted environment.

Review Renaissance's privacy policies at bit.ly/RenaissancePrivacy.

Vigorous network security procedures and appliances protect customers' data from electronic intrusion. These include antivirus software; firewalls; regular patching, updating, and hardening processes; and application security to ensure connectivity protection. Renaissance performs full-system scans on a regular schedule and updates antivirus signatures as they are released. We follow stringent data backup and recovery protocols to protect our customers.

Renaissance tracks an array of metrics, including log files, access logs, system usage, and network bandwidth consumption. We monitor all hosted servers 24 hours a day, 7 days a week, using various physical and automated methods. Any suspicious activity is promptly investigated and addressed. Our risk management plan ensures our company stays up to date on information including security best practices, government policy and legislation, threats and vulnerabilities, and new technologies. Boundary protection is in place on all systems with a connection to an untrusted network. A protective monitoring regime tracks how our information and communications technology systems are used. We also protect these systems from malicious and mobile code.

We prohibit advertising on our hosted sites, which means there are no opportunities for third-party vendors to target advertising to the educators or students who use our solutions. At no time will Renaissance sell, distribute, release, or publish customer information to a third party without prior written consent from the data's owner. Parents, legal guardians, and eligible students who seek access to review or amend records only may do so through the school or educational entity that owns the data. Should a school wish to share its Renaissance-generated data with a third party, such as another application provider or a government agency, the school must initiate that process.

Fewer than 10 percent of Renaissance's employees have access to the production environment in which our customers' personally identifiable information is kept. Network security boundaries, also known as segmentation, are defined and enforced to limit access to customer data. All Renaissance employees and approved agents must sign a legally enforceable nondisclosure agreement prior to the start of their tenure or project. These workers are obligated to protect all data and ensure its security, including immediately reporting any suspected or known security breaches, data theft, unauthorized release, or unauthorized interception of customer data.

It is exceedingly rare that third-party contractors come into contact with any of the personally identifiable information Renaissance maintains. Third-party contractors that could potentially have access to the hosted environment where personally identifiable information resides are Amazon Web Services (application hosting provider), Wisconsin Independent Networks (data center co-location provider), or firms that Renaissance shires to conduct independent security reviews, audits, and penetration and vulnerability. Policies, standards, and certifications spell out data privacy expectations

At all times, Renaissance complies with key security and confidentiality records, laws, and guidelines, including applicable requirements of the Family Educational Rights and Privacy Act (FERPA), Children's Online Privacy and Protection Act (COPPA), the Children's Internet Protection Act (CIPA, CIPA-2), the Health Insurance Portability and Accountability Act (HIPAA), and the General Data Protection Regulation (GDPR). Renaissance also follows the IT Internal Governance's Institute's guidelines on internal governance and operations of our systems and the Payment Card Industry Data Security Standards for processing credit card information. All Renaissance information security and privacy policies and standards are formalized, documented, reviewed, and updated at least annually. Policies related to data privacy are available for review online.

If you have more questions about Renaissance's privacy policies and data security measures, e-mail privacy@renaissance.com.

Renaissance chose to sign the Student Data Privacy Pledge http://studentprivacypledge.org) because our company believes that protecting student privacy is of paramount significance. First and foremost, we don't allow advertising on our hosted sites. This means there is no opportunity for third-party vendors to target advertising to the teachers or students who use our solutions.

Our data protection and security practices align with those identified by the pledge, including enforcing strict limits on data retention; providing comprehensive security; ensuring transparency about the data we collect and how we use it; using data for authorized educational purposes only; notifying and gaining customer consent prior to making material changes to our privacy policies; and prohibiting the sale of student information

The legally binding commitments in the pledge can be enforced by United States' Attorneys General and the Federal Trade Commission, which ensures these protections extend to our international customers. The Federal Trade Commission works with more than 100 foreign competition and consumer protection authorities around the world, and cooperates with foreign authorities on enforcement and policy matters through formal and information agreements. The U.S. SAFE WEB Act enables these international consumer protection tools.[1]

The Federal Trade Commission also oversees the U.S.-E.U. Privacy Shield Framework, with which Renaissance also is certified. The U.S.-E.U. Privacy Shield Framework was designed to provide companies with a mechanism to comply with data protection requirements when transferring personal data internationally. Organizations must publicly disclose their privacy policies to individuals, provide free and accessible dispute resolution, cooperate with the U.S. Department of Commerce, maintain data integrity for as long as that data is held, take accountability for any data it transfers to third parties, and maintain transparency related to any enforcement actions. Self-certification is completed annually. For more information, please visit http://bit.ly/PrivacyShield_Renaissance.

[1] "International Consumer Protection." International Consumer Protection | Federal Trade Commission. U.S. Federal Trade Commission. Web. <https://www.ftc.gov/policy/international/international-consumer-protection>.

RENAISSANCE®