

Weld County School District 6 Data Protection Agreement

This Data Protection Agreement is attached to and forms a part of the Renaissance Quotes dated August 6, 2018, by and between Weld County School District 6 (“District”) and Renaissance Learning (“Vendor”). This Agreement supersedes the Contract by adding to, deleting from and modifying the Contract as set forth herein. To the extent any such addition, deletion or modification results in any conflict or inconsistency between the Contract and this Agreement, this Agreement shall govern and the terms of the Contract that conflict with this Agreement or are inconsistent with this Agreement shall be of no force or effect.

1. Definitions

a. “Anonymized Data” means De-identified Data, as defined below, which does not include a record code and cannot be linked to the original data source.

b. “Authorized Persons” means Vendor’s employees or subcontractors who have a need to know and will access District Data to enable Vendor to perform its obligations under this Agreement.

c. “De-identification” means the process of removing or obscuring all identifiable information until all data that can lead to individual identification has been expunged or masked. Simple removal of direct identifiers from data does not constitute adequate de-identification. District Data that has undergone sufficient De-identification shall be referred to as De-identified Data.

d. “District Data” means information, including, but not limited to, Personally Identifiable Information, business, administrative and financial information, intellectual property information, and other information that is not intentionally made generally available by the District on public websites or publications, that is provided to Vendor by or at the direction of District in the course of Vendor’s performance under this Agreement. “District Data” includes metadata and data derived from the use of District Data and metadata.

e. “End User” means the individuals authorized by the District to access and use the Services provided by the Vendor under this Agreement.

f. “Personally Identifiable Information” or “PII” shall mean District Data that, alone or in combination, is linked or linkable to a specific student or person that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student or person with reasonable certainty. PII includes, but is not limited to, a student’s name; the name of a student’s parent; guardian or other family member; the address of a student or a student’s family; a personal identifier such as a student’s social security number, student number, or biometric record; other indirect student identifiers such as a student’s date of birth, place of birth, or mother’s maiden name; and various demographic attributes, such as race, socioeconomic information, and gender. To the extent it is not already included in the definition hereinabove, PII also includes “personal information” as defined in the Colorado Open Records Act, C.R.S. 24-72-101 *et seq.*; personally identifiable

information contained in student “education records” as that term is defined in the Family Educational Rights and Privacy Act, 20 U.S.C. 1232g; “protected health information” as that term is defined in the Health Insurance Portability and Accountability Act, 45 C.F.R. Part 160.103; “nonpublic personal information” as that term is defined in the Gramm-Leach-Bliley Financial Modernization Act of 1999, 15 U.S.C. 6809; credit and debit card numbers and/or access codes and other cardholder data and sensitive authentication data as those terms are defined in the Payment Card Industry Data Security Standards; other financial account numbers, access codes, and state- or federal-identification numbers such as driver’s license, passport or visa numbers.

g. “Securely Destroy” means taking actions that render data written on physical or electronic media unrecoverable by both ordinary and extraordinary means.

h. “Security Breach” means an event in which District Data is exposed to unauthorized disclosure, access, alteration or use or a system configuration that results in unsecured disclosure, access, alteration or use, such as a failed firewall or password disclosure.

i. “Services” means any good or services acquired by the District from the Vendor, including, but not limited to, computer software, mobile applications (apps), and web-based tools accessed by students and/or their parents through the Internet or on a hard drive of a computer or electronic device and used for educational purposes.

j. “Mining District Data” means to search through, analyze, access, or extract District Data, metadata, or information that is not necessary to accomplish the Services or purpose(s) of this Agreement for the benefit of the District.

2. Rights and License in and to District Data

District retains all right, title, and interest in and to the District Data, including without limitation all now known or hereafter existing rights associated with works of authorship, including copyrights and moral rights; trademarks or service mark rights; trade secret rights; patents and patent rights; and all other intellectual property (collectively referred to as “Intellectual Property”). For the term of this Agreement, unless sooner terminated, Vendor shall have a limited, nonexclusive license to use the District Data and Intellectual Property solely for the purpose of performing its obligations hereunder. This Agreement does not give Vendor any rights, title, or interest, implied or otherwise, to District Data or Intellectual Property, except as expressly stated in the Agreement. District shall have the right to access and retrieve District Data stored by or in possession of Vendor at any time upon written notice to Vendor.

3. Data Privacy

a. Vendor will use District Data only for the purpose of performing the Services and fulfilling its duties under this Addendum and will not use, sell, rent, transfer, distribute, alter, mine, or disclose such data, including Anonymized Data, to any third party without the prior written consent of the District, except as required by law. If District consents in writing to Vendor’s use of Anonymized Data, then Vendor agrees not to attempt to re-identify the Anonymized Data.

b. District Data will not be stored outside the continental United States unless Vendor has given the District advance written notice of where and how the servers are housed and managed and the District has consented in writing to such storage.

c. Vendor will provide access to District Data, including De-identified Data, only to its Authorized Persons. Vendor will ensure that all Authorized Persons have received and understood appropriate instruction as to how to comply with the data protection provisions of this Agreement. Upon District's written request, Vendor shall promptly identify in writing all Authorized Persons as of the date of such request. Vendor shall at all times cause such Authorized Persons to abide strictly by Vendor's obligations under this Agreement. Vendor further agrees to maintain a disciplinary process, up to and including termination, to address any unauthorized use, modification or disclosure of District Data by any Authorized Persons.

d. Vendor warrants and represents that during the five-year period preceding the Effective Date of the Agreement, it has not been found in violation of FERPA by the Family Policy Compliance Office.

e. With the exception of De-identified Data that the District has agreed in writing to allow Vendor to use, Vendor will not use District Data for its own commercial benefit, including but not limited to, advertising or marketing purposes, unless such use is specifically authorized by this Agreement or otherwise authorized in writing by the District.

f. In performance of the Services required by the Agreement, Vendor may collect personal information (as defined in the Children's Online Privacy and Protection Act of 1998, 5 U.S.C. 6501 to 6505 and its implementing regulations) from children under thirteen years of age. Vendor warrants, represents, and covenants that such collection is and shall be for the use and benefit of the District and for no other commercial purpose. Vendor has provided District with full notice of its collection, use, and disclosure practices.

g. Vendor is prohibited from building a personal profile of a student or Mining District Data for any purposes other than those agreed to by the Parties; provided, however, Vendor is not prohibited from using District Data for purposes of adaptive learning or customized education when used solely for the purpose of performing the Services or its obligations hereunder.

h. Upon District's written request, to confirm Vendor's compliance with this Agreement and/or any applicable laws, regulations, and/or industry standards, Vendor shall provide District with the most recent copy of the Vendor's network security audit.

4. Data Security

a. Vendor will store and process District Data in accordance with commercial best practices, including implementing appropriate administrative, physical, and technical safeguards that are no less rigorous than those outlined in FIPS PUB 200, to secure such data from unauthorized access, disclosure, alteration, and use. Vendor shall ensure that all such safeguards, including the manner in which District Data is collected, accessed, used, stored, processed, disposed of and disclosed, comply with all applicable

federal and state data protection and privacy laws, regulations and directives, as well as the terms and conditions of this Addendum. Without limiting the foregoing, and unless expressly agreed to the contrary in writing, Vendor warrants that all electronic District Data will be:

- i. encrypted at 128-bit level in transmission using SSL (Secure Sockets Layer) and
- ii. stored at no less than 128-bit level encryption.

b. Upon request, Vendor will provide District certification indicating that an independent vulnerability or risk assessment of the Vendor's data security program has occurred.

5. Security Breach

a. *Response.* Immediately upon becoming aware of a Security Breach, a complaint of a Security Breach or of circumstances that could have resulted in unauthorized access to or disclosure or use of District Data, Vendor will notify the District in writing, fully investigate the incident, cooperate fully with the District's investigation of and response to the incident, and use best efforts to prevent any further Security Breach at Vendor's expense in accordance with applicable privacy laws. Except as otherwise required by law, Vendor will not provide notice of the incident directly to individuals whose Personally Identifiable Information was involved, regulatory agencies, or other entities, without prior written permission from the District.

b. *Liability.* In addition to any other remedies available to the District under law or equity, Vendor will reimburse the District in full for all costs incurred by the District in investigation and remediation of any Security Breach caused in whole or in part by Vendor or Vendor's Authorized Persons, including but not limited to providing notification to individuals whose Personally Identifiable Information was compromised and to regulatory agencies or other entities as required by law or contract; providing one year's credit monitoring to the affected individuals if the Personally Identifiable Information exposed during the breach could be used to commit financial identity theft; and the payment of legal fees, audit costs, fines, and other fees imposed against the District as a result of the Security Breach.

6. Response to Legal Orders, Demands or Requests for Data

a. Except as otherwise expressly prohibited by law, Vendor will immediately notify the District of any subpoenas, warrants, or other legal orders, demands or requests received by Vendor seeking District Data; consult with the District regarding its response; cooperate with the District's reasonable requests in connection with efforts by the District to intervene and quash or modify the legal order, demand or request; and, upon the District's request, provide the District with a copy of its response.

b. If the District receives a subpoena, warrant, or other legal order, demand (including any request pursuant to the Colorado Open Records Act) or request seeking District Data maintained by Vendor, the District will promptly notify Vendor and Vendor will promptly supply the District with copies of the District Data for the District to respond.

c. Vendor agrees to fully cooperate, at its own expense, with District in any third party litigation or other formal action the District reasonably deems necessary to protect its rights relating to the use, disclosure, protection and maintenance of District Data as required under applicable law.

7. Data Transfer Upon Termination or Expiration

With the exception of De-identified District Data that District has specifically agreed in writing to allow Vendor to use after termination or expiration of the Agreement, upon termination or expiration of the Agreement, Vendor will ensure that all District Data is securely returned or destroyed as directed by the District. Transfer to the District or a third party designated by the District shall occur within a reasonable period of time but no later than thirty (30) days after expiration or termination of the Agreement, and without significant interruption in service or access. Vendor shall ensure that such transfer/migration uses facilities and methods that are compatible with the relevant systems of the District or its transferee, and to the extent technologically feasible, that the District will have reasonable access to District Data during the transition. In the event that the District requests destruction of its data, Vendor agrees to Securely Destroy all data in its possession and in the possession of any Authorized Persons to which the Vendor might have transferred District Data. The Vendor agrees to promptly certify in writing to District that such District Data has been returned to District or disposed of securely.

8. Audits

The District reserves the right in its sole discretion to perform audits of Vendor at the District's expense to ensure compliance with the terms of this Agreement and all applicable laws, regulations, and industry standards. The Vendor shall reasonably cooperate in the performance of such audits.

9. No End User Agreements

This Agreement is the entire agreement between the District (including End Users) and the Vendor. In the event that the Vendor enters into terms of use agreements or other agreements or understandings, whether electronic, click-through, verbal or in writing, with End Users, the parties agree that in the event of a conflict between the terms of any such agreement and this Agreement, the terms of this Addendum and the Contract, in that order of precedence, shall control.

10. Transparency

Within ten (10) business days after signing this Agreement, to the extent not previously provided, Vendor shall make available to District the following information about its products or services, as applicable: (a) type of PII that is collected or generated by the Vendor or disclosed to a third party; (b) the educational purpose for which the PII is used; (c) Vendor's policies regarding retention and disposal of PII; and (d) type of information, including but not limited to PII, that is collected and how it is shared or used. In addition, Vendor shall notify District prior to changing its privacy policies and shall cooperate with any students or parents who request a reasonable correction of student information created or maintained by Vendor.

11. School Service Contract Provider

If Vendor is a “school service contract provider” as defined in the Colorado Student Data Transparency and Security Act, C.R.S. §§ 22-16-101 to -112, then Vendor shall comply with the requirements set forth in C.R.S. §§ 22-16-108, -109, and -110.

12. Termination

Subject to Section 15, this Addendum will automatically terminate without any further action of the Parties upon the termination or expiration of the Contract between the Parties.

13. Indemnification

Vendor shall indemnify and hold District and its directors, employees, board members and agents from and against all losses, damages, liabilities, deficiencies, actions, judgments, interest, award, penalties, fines, costs or expenses, including attorneys’ fees, the costs of enforcing any right to indemnification hereunder and the cost of pursuing any insurance providers, arising out of or resulting from any third-party claim against District or its directors, employees, board members and agents arising out of or resulting from Vendor’s failure to comply with any of its obligations under this Addendum. These indemnification duties shall survive termination or expiration of the Agreement.

14. Insurance

Vendor shall purchase and maintain during the term of this Agreement Technology Errors and Omissions/Professional Liability Insurance, including Network Security and Privacy Liability Insurance. Such policy shall cover professional misconduct or lack of ordinary skill in providing services, systems and/or product as defined in the scope of services of this Agreement. In the event that the professional liability insurance required by this Agreement is written on a claims-made basis, Vendor warrants that any retroactive date under the policy shall precede the effective date of this Agreement; and that either continuous coverage will be maintained or an extended discovery period will be exercised for a period of two (2) years beginning at the time work under this Agreement is completed. If such insurance is maintained on an occurrence form basis, Vendor shall maintain such insurance for an additional period of one (1) year following termination of Agreement. If such insurance is maintained on a claims-made basis, Vendor shall maintain such insurance for an additional period of three (3) years following termination of the Agreement. If Vendor contends that any of the insurance it maintains pursuant to other sections of this clause satisfies this requirement (or otherwise insures the risks described in this section), then Vendor shall provide proof of same. The insurance shall provide coverage for the following risks:

a. Any error, misstatement, misleading statement, act, omission, neglect, breach of duty or personal injury offense for the Vendor rendering or failure to render technology services and the failure of the Vendor’s technology products to perform the function or serve the purpose intended.

b. Liability arising from theft, dissemination and/or use of District Data stored or transmitted in electronic form.

c. Network Security Liability arising from the unauthorized access to, use of or tampering with computer systems including hacker attacks, inability of an authorized third party, to gain access to Vendor's services including denial of service, unless caused by a mechanical or electrical failure.

d. Liability arising from the introduction of a computer virus into, or otherwise causing damage to, a customer's or third person's computer, computer system, network or similar computer related property and the data, software, and programs thereon.

In addition to the foregoing requirements, the policy shall provide a waiver of subrogation in favor of the District and shall be endorsed to include the following additional insured language: "Weld County School District 6, and its elected officials, trustees, employees, and agents, shall be named as additional insureds with respect to liability arising out of the activities performed by, or on behalf of the Vendor." The policy shall be for the following amounts:

For Agreements of \$500,000 or less

Minimum Limits:

Per Loss	\$	1,000,000
Aggregate	\$	3,000,000

For Agreements over \$500,000

Minimum Limits:

Per Loss	\$	3,000,000
Aggregate	\$	5,000,000

15. Survival

The Vendor's obligations under Sections 3, 4, 5, 7, 8, 11, 13, and 14 shall survive termination of the Agreement until all District Data has been returned or Securely Destroyed.

[Signature page appears on next page]

IN WITNESS WHEREOF, the parties have executed this Addendum contemporaneously with the Contract.

WELD COUNTY SCHOOL DISTRICT 6


VENDOR

By: Mandy Hydock, Director of Finance

By: Renaissance Learning, Inc.
Legal Name of Vendor

Date: Aug 30, 2018

39-1559474
FEIN


Signature of Authorized Officer

Dir of Information Security
Title of Authorized Officer

Date: 8/30/2018



Application and Hosting Privacy Policy (US Applications)

Renaissance Learning, Inc. and its subsidiaries (collectively, "Renaissance") consider the privacy and security of its Users of its Applications and Hosting Services to be of paramount importance. Renaissance has developed this Application and Hosting Privacy Policy (this "Policy") to inform Users of its policies and procedures regarding the collection, use and disclosure of Personally Identifiable Information and non-personal information Renaissance receives from Schools and Users. Nothing in this Policy shall be construed as granting any School or User any rights to use or access any Application or Hosting Services and any School or User shall only have the right to use and access the Applications as set forth in the agreement(s) entered into between a User's School and Renaissance (the "License and Services Agreement").

Definitions

"Applications" means the commercial educational online software products being provided to a School under such School's License and Services Agreement.

"User" means any user of the Applications and Hosting Services.

"Hosting Services" means the hosting services that Renaissance provides to a School to host the Applications as set forth in such School's License and Services Agreement. Hosting Services can include access to Applications via the world wide web.

"Non-Personally Identifiable Information" means information about a User that is not considered Personally Identifiable Information as defined below.

"Personally Identifiable Information" means information about a User that can be used on its own or with other information to identify, contact, or locate a single individual, including, but not limited to, the following:

- Any information that can be used to distinguish or trace an individual's identify such as full name, social security number, date and place of birth, mother's maiden name, or biometric records;
- Any other information that is linked or linkable to an individual such as medical, educational, financial, and employment information;
- Two or more pieces of information that separately or when linked together can be used to reasonably ascertain the identity of the person.

"School" means a school district, public or private school, after school service provider, library or other educational organization or learning center that provides educational services that, in all cases, license any Applications from Renaissance.

School Controls Personally Identifiable Information

RENAISSANCE®

The collection, input, use, retention, disposal, and disclosure of any Personally Identifiable Information submitted by Users via the Applications to the Hosting Services are controlled solely by the School. The School is responsible for providing all necessary notices and obtaining all necessary consents from Users to collect, use, disclose and submit the Personally Identifiable Information via the Applications or Hosting Services for Renaissance to use in accordance with the License and Services Agreement. Renaissance will not delete, change, or divulge any Personally Identifiable Information from its Applications or Hosting Services controlled by the School except as outlined in this Policy. To the extent a User has questions regarding the privacy associated with the Applications licensed by a User's School, please contact the School. Also, should a User wish to revoke their consent, or "opt-out" of a particular use of their Personally Identifiable Information, please contact the User's School.

What Information Renaissance Collects and Maintains

Renaissance Collects and Maintains the following information:

- Usage Details. When Users access the Applications or Hosting Services, Renaissance may automatically collect certain details of the User's access to and use of the Applications and Hosting Services, including traffic data, location data, logs and other communication data and the resources that Users access and use on or through the Applications or Hosting Services. This information is Non-Personally Identifiable Information that is aggregated.
- Cookies (or mobile cookies) and Web Beacons. A cookie is a small file placed on computing devices such as computers, tablets, and smartphones. A web beacon is a small electronic file such as a clear gif, pixel tag, or single-pixel gif. Renaissance may use cookies and web beacons to collect usage details. It may be possible to refuse to accept cookies and web beacons by activating the appropriate setting on the computing devices. However, selection of this setting may disable access certain parts of the Applications or Hosting Services. The information collected via cookies and web beacons is Non-Personally Identifiable Information that is aggregated.
- Device Information. Renaissance may collect information about a User's computer device, mobile device, and Internet connection, including the device's unique device identifier, IP address, operating system, browser type, and mobile network information. This information is Non-Personally Identifiable Information that is aggregated.
- Stored Information and Files. The Applications or Hosting Services may access metadata and other information associated with other files stored on a User's device (for example, to provide access to an e-Book or other store material). This information is Non-Personally Identifiable Information that is aggregated.
- Information input by Users. Users input information to the Applications and Hosting Services such as salutation, name, user name and password, name of School, ID number, gender, grade, state student ID, state personnel ID, primary position, date of birth, ethnicity and language, as well as assessment responses, comprehension quizzes, lesson completion, practice and other academic skills that is then stored by the Application and Hosting Services. This information may contain Non-Personally Identifiable Information as well as Personally Identifiable Information.
- Information generated from using the Applications and Hosting Services. Users' use of the Applications and Hosting Services generates information or outputs such as calculated scores for assignments, assessments and quizzes, as well as information contained within custom reports, which combine information input by Users and calculated scores. This information may contain Non-Personally Identifiable Information as well as Personally Identifiable Information.

How Renaissance Uses Information Collected

RENAISSANCE®

Renaissance only uses the information, including Personally Identifiable Information, it collects pursuant to this Policy. The most common of those uses are as follows:

- To provide School and Users with access to the Applications and the Hosting Services and their contents, and any other information, products or services that School requests from Renaissance.
- To communicate with Users as necessary to fulfill Renaissance's obligations to Schools.
- To provide School notices about its account, including expiration and renewal notices.
- To carry out the School's and Renaissance's respective obligations and enforce Renaissance's rights arising from the License and Services Agreement, including for billing and collection.
- To notify School of changes to any products or services Renaissance offers or provides through it.
- To estimate School size and usage patterns.
- To store information about School preferences, allowing Renaissance to customize its services.

In addition, Renaissance aggregates information it collects, including Non-Personally Identifiable Information and uses such aggregated information and other Non-Personally Identifiable Information it collects as follows:

- To maintain and improve performance or functionality of the Applications and the Hosting Services.
- To demonstrate the effectiveness of Renaissance's products, including, without limitation, the Applications and the Hosting Services.
- For general research and to research and develop new technologies.

What Personally Identifiable Information Renaissance Discloses

Renaissance may disclose Non-Personally Identifiable Information, including the Non-Personally Identifiable Information from the aggregated Personally Identifiable Information about Users of its Applications and the Hosting Services.

In addition, Renaissance may disclose Personally Identifiable Information as described in this Policy. Generally, Renaissance may disclose Personally Identifiable Information under the following circumstances:

- Renaissance may share Personally Identifiable Information with third-party contractors to support Renaissance's operations of the Applications and Hosting Services who are bound by contractual or other obligations to use the information only for such purpose and to keep the information confidential. Third parties are prohibited from using Personally Identifiable Information to engage in targeted advertising.

Name of third-party contractor ("Recipient") (Telephone No.)	Country where Recipient is Located	Recipient's Purpose for Using the Personally Identifiable Information (Description of delegated work scope)	Items of Personally Identifiable Information to be Transferred	Time and Method of Transfer	Recipient's Period of Retention and Use
Amazon Web Services (866-216-1072)	Seattle, Washington, USA	Application hosting	Please refer to the information	On an as-needed basis through	Until the Recipient's purpose for

RENAISSANCE®

Wisconsin Independent Network, LLC (866-206-2027)	Eau Claire, Wisconsin, USA	Data center co- location	listed in the section above entitled "What Information Renaissance Collects and Maintains"	information and communication networks	using the personal information has been fulfilled
--	----------------------------------	-----------------------------	--	---	---

- Renaissance may share Personally Identifiable Information if it is required to do so by law or legal process, such as to comply with any court order or subpoena or to respond to any government or regulatory request.
- Renaissance may share Personally Identifiable Information if it reasonably believes disclosure necessary or appropriate to protect the rights, property or safety of Renaissance, its customers or to enable Renaissance to take precautions against liability.
- Renaissance may share Personally Identifiable Information with law enforcement agencies or for an investigation related to public safety.
- Renaissance may sell, transfer, or otherwise share some or all of its assets, including the Personally Identifiable Information it collects, in connection with a merger, acquisition, reorganization or sale of assets or in the event of bankruptcy, in which case the successor entity is subject to the same commitments set forth in this Policy.
- Renaissance may share Personally Identifiable Information with third-parties that a School has authorized.

Renaissance will not use Personally Identifiable Information to conduct targeted advertising to students. Renaissance does not publicly disseminate Personally Identifiable Information submitted by Users. Renaissance permits Users to share comments and ratings between classmates and teachers within the Applications. Renaissance does not publicly disseminate those comments and ratings.

Do Not Track

Certain browsers have settings that allow you to turn on a "Do Not Track" ("DNT") feature. Renaissance Place service does not support DNT in order that we may provide the service to authenticated users. We do not intentionally or knowingly allow other parties to collect Personally Identifiable Information and have security measures in place to prevent third parties from collecting information about your Renaissance Place activities.

Exercise of Right to Disclosure, Alternation, Addition, Cessation of Use, and Deletion of Personally Identifiable Information

Any User or parents of such User if a User is a minor may review and amend any Personally Identifiable Information of such User by contacting the School and following the School's procedures for amending such User's Personally Identifiable Information. Renaissance will not make any changes to any Personally Identifiable Information without the applicable School's express written permission, and then only in accordance with applicable Privacy Laws.

Data Retention and Destruction

RENAISSANCE®

When the School terminates its subscription to the Applications and Hosting Services, all Personally Identifiable Information of Users that was collected, used, disclosed and submitted via the Applications and Hosting Services will be removed from the Applications. Personally Identifiable Information removed from the Applications will be removed from Renaissance's primary data center after 30 days and will be removed from all backups within 90 days of the removal from the Applications. However, to the extent that any Personally Identifiable Information must be retained under applicable laws and regulations, the Personally Identifiable Information will be retained and used for the period and purpose as prescribed under such laws and regulations.

When removing Personally Identifiable Information, Renaissance shall take technically reasonable measures to make the Personally Identifiable Information irrecoverable or irreproducible as follows:

- (i) electronic files containing Personally Identifiable Information shall be irrecoverably deleted using an appropriate technical method; and
- (ii) any other records, print-outs, documents or any other recording media shall be shredded or incinerated.

Security

Personally Identifiable Information is stored in databases maintained by Renaissance or its service providers. Databases for Users inside the United States are stored on servers located in the United States and databases for other Users may be stored on servers located inside or outside of the United States or other countries. Renaissance may use third-party storage or service-provider companies to store Personally Identifiable Information, for which Personally Identifiable Information for Users in the United States will be in the United States and Personally Identifiable Information for other Users may be inside or outside of the United States.

We have taken certain physical, technical, contractual and administrative steps to protect the confidentiality, security and integrity of Personally Identifiable Information. However, no method of transmission over the Internet or method of electronic storage is completely secure and we cannot guarantee its absolute security. It is a User's responsible to maintain the confidentiality of his or her account information.

Links to Other Websites and Services

Users accessing the Applications and Hosting Services may find links to websites and applications owned and operated by other organizations. Please note that when you click on one of these links, you are moving to another website and that the content of those linked sites is the responsibility of the organization actually owning and/or operating the site or application. Renaissance is not responsible for, and has no control over, the content or privacy policy of any linked site. Renaissance encourages Users to read the privacy statements of any linked site as its privacy policy may differ from Renaissance's.

Local Laws

To the extent applicable to a User, the following applies to such User and will control in the event of conflict with preceding sections of this Policy:

Korea

Nothing in this Policy shall be construed as granting any School or User any rights to use or access any Application or Hosting Services and any School or User shall only have the right to use and access the Applications as set forth in the agreement(s) entered into between a User's School and TIME Education Co.



Ltd. ("TIME") (the "License Agreement"). Any references to the "License and Services Agreement" in preceding sections of this Policy shall be construed as referring to the License Agreement between a User's School and TIME.

Control of Personally Identifiable Information

The collection, input, use, retention, disposal, and disclosure of any Personally Identifiable Information submitted by Users via the Applications to the Hosting Services are controlled by Renaissance and TIME. Personally Identifiable Information submitted by Users via the Applications to the Hosting Services is sent on an as-needed basis via information and communication networks to databases maintained by Renaissance in the United States. (For more information on the items of Personally Identifiable Information being stored, purpose of storage, and duration of storage, please refer to the sections entitled What Information Renaissance Collects and Maintains, How Renaissance Uses Information Collected, and Data Retention and Destruction.) The School is responsible for providing all necessary notices and obtaining all necessary consents from Users to collect, use, disclose and submit the Personally Identifiable Information via the Applications or Hosting Services for Renaissance and TIME to use in accordance with the agreement entered into between the school and the TIME. Renaissance and TIME will not delete, change, or divulge any Personally Identifiable Information from its Applications or Hosting Services except as outlined in this Policy.

Exercise of Right to Disclosure, Alternation, Addition, Cessation of Use, and Deletion of Personally Identifiable Information

Please contact Renaissance directly in relation to a request for the disclosure, alternation, addition, cessation of use, or deletion of Personally Identifiable Information held by Renaissance. If you are under the age of 14, your legal guardian must take the above action with respect to your Personally Identifiable Information. In view of maintaining accuracy and security and preventing the leakage of Personally Identifiable Information, in the absence of a special procedure pursuant to applicable laws or regulations, any necessary confirmation shall be conducted without delay. In the event of non-performance or delay in completing the request, Renaissance will strive to provide an explanation for the cause of the delay.

What Collected Information Renaissance Discloses

Renaissance shares the following Personally Identifiable Information of a User with such User's School for the purpose of assessing and monitoring the User's use of the educational online software products until such purpose has been fulfilled: User's name, user name and password, name of School, ID number, gender, grade, state student ID, date of birth, ethnicity and language, assessment responses, comprehension quizzes, lesson completion, practice, and other academic skills, as well as calculated scores for assignments, assessments and quizzes, and information contained within custom reports.

United States

Family Education Rights and Privacy Act

- The Family Education Rights and Privacy Act of 1994 and the regulations thereunder (collectively, "FERPA"), impose onto "educational agencies or institutions", obligations and restrictions, including, without limitation obligations and restrictions with respect to
 - the handling and disclosure of Personally Identifiable Information contained in the educational records an educational agency or institution maintains regarding its students,
 - any data that may be accessed, obtained, received, extracted or otherwise used by Renaissance (or which may be disclosed in any manner to Renaissance by or on behalf of

RENAISSANCE®

an educational agency or institution), in individualized or aggregate form, in connection with an educational agency or institution's use of the Applications and the Hosting Services as well as any services provided by Renaissance in connection with the Applications and the Hosting Services.

- Renaissance agrees to adhere to the disclosure requirements under FERPA and will not disclose any Personally Identifiable Information from the Application's database to any third party except: (i) if required by law or valid court order or (ii) as permitted elsewhere in the Agreement or this Policy, where the third party is bound by contractual or other obligations to use the information only for such purpose and to keep the information confidential. Renaissance will cooperate with the School with respect to the School's disclosure requirements; all such disclosures shall be through the School.
- Third parties who contract with Renaissance are contractually prohibited from using Personally Identifiable Information from the Application's database to engage in targeted advertising.

Children's Online Privacy Protection Act

- The Children's Online Privacy Protection Act and the regulations thereunder (collectively, "COPPA") impose requirements on operators of commercial websites and online services directed to children under 13 ("operators," such as Renaissance) to provide direct notice to parents about their practices for collecting, using and disclosing Personally Identifiable Information from children under the age of 13 ("children"). COPPA also requires operators to obtain verifiable parental consent prior to the collection of Personally Identifiable Information from children.
- School, to the extent necessary for use of the Applications and Hosting Services, is required to provide direct notice of this Policy to parents of children under the age of 13 and to obtain the requisite parental consent, as a condition of using the Hosting Services and Applications.
- In accordance with COPPA, Renaissance agrees not to share, sell, rent or transfer children's Personally Identifiable Information other than as described in the Agreement and this Policy.

International Transfer

Personally Identifiable Information may be transferred to—and maintained on—computers located outside of a User's state, province, country or other governmental jurisdiction where privacy laws may not be as protective as those in a User's jurisdiction. If a User is located outside of the United States and provides Personally Identifiable Information to Renaissance through the Applications and Hosting Services, Renaissance transfers information to the United States and processes it there. As stated above, the School is responsible for providing all necessary notices to and obtaining all necessary consents from Users to transfer User information to the United States and allow Renaissance to process it there. To the extent a User has questions regarding the notice or consent to transfer his or her Personally Identifiable Data to Renaissance for use in connection with this Policy, please contact the School.

EU – U.S. Privacy Shield

Renaissance participates in and complies with the EU-U.S. Privacy Shield Framework (the "Framework"). Renaissance has certified that it adheres to the Privacy Shield Principles of Notice; Choice; Accountability for Onward Transfer; Security; Data Integrity and Purpose Limitation; Access; and Recourse, Enforcement and Liability. If there is any conflict between this Policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield Framework, visit <https://www.privacyshield.gov/>. To view our certification, visit the [U.S. Department of Commerce's Privacy Shield List](#).

Renaissance is responsible under the Framework for the processing of Personally Identifiable Information

RENAISSANCE®

it receives. For Personally Identifiable Information transferred from the EU, if Renaissance transfers a User's Personally Identifiable Information to a third party, Renaissance will ensure that the third party is contractually obligated to process such User's Personally Identifiable Information only for limited, specific purposes consistent with this Policy. Renaissance will also ensure that the third party will apply the same level of protection to that data as the EU-U.S. Privacy Shield Principles and will notify Renaissance if it makes a determination that it can no longer meet this obligation. Renaissance also complies with the Privacy Shield Principles for the onward transfer liability provisions.

With respect to Personally Identifiable Information received or transferred pursuant to the Framework, Renaissance is subject to the regulatory enforcement powers of the U.S. Federal Trade Commission. In certain situations, Renaissance may be required to disclose Personally Identifiable Information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

In compliance with the EU-U.S. Privacy Shield, Renaissance strives to resolve all complaints about privacy and the collection or use of User's information. If you have questions about our participation in the Privacy Shield program or have a complaint, please send an email to privacy.officer@renaissance.com. If you have any unresolved privacy or data use concern that we have not addressed satisfactorily, please contact our U.S.-based third party dispute resolution provider [JAMS](#).

Under certain conditions, more fully described on the Privacy Shield website at <https://www.privacyshield.gov/article?id=How-to-Submit-a-Complaint>, you may invoke binding arbitration when other dispute resolution procedures have been exhausted.

Updates

Renaissance may revise this Policy from time to time and will make an updated version of this Policy available on a publicly accessible location. Subject to the foregoing, Renaissance will not make material changes to this Policy, without first providing prominent notice to School allowing it choices before data is used in any manner inconsistent with terms as they were initially provided; and not make material changes to other policies or practices governing the use of Personally Identifiable Information that are inconsistent with contractual requirements except as required by law. Notwithstanding the foregoing, should laws and regulations change to further restrict the collection, use, and distribution of Personally Identifiable Information, Renaissance shall be permitted to make appropriate changes to this Policy to comply with the laws and regulations without issuing prior notice to School or any User.

Website Privacy Policies

The Applications and Hosting Services may contain links to other companies' websites and services that may or may not have privacy policies of their own. Renaissance is not responsible for the privacy practices of others and we recommend you determine if they have a privacy policy and read it. Renaissance has websites with separate privacy policies. Those policies shall remain in place notwithstanding this Policy.

Contact Renaissance

If you have any questions about this Policy or how Renaissance collects, uses, and shares Personal Identifiable Information, please contact Renaissance using the information below:

ATTN: Privacy Officer

Jeff Christensen – Director, Information Security



Renaissance Learning Inc.

PO Box 8036

2911 Peach Street

Wisconsin Rapids, Wisconsin 54495-8036

Toll Free: (800)338-4204

privacy.officer@renaissance.com

A Spanish translation of this Policy is available [here](#).