

BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY - SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION

Pursuant to Education Law § 2-d and Section 121.3 of the Commissioner's Regulations, the educational Agency (EA) is required to post information to its website about its contracts with third-party contractors that will receive Personally Identifiable Information (PII).

Name of Contractor	Renaissance Learning, Inc. Brennan Middle School - Flocabulary and Nearpod 11/1/26- 10/31/27 James E Allen Jr/Sr High School - Flocabulary 11/1/26-10/31/27
PII Declaration	Does your organization/software collect student personally identifiable information (PII) or staff PII? Examples of student PII: a. The student's name; b. The name of the student's parent or other family members; c. The address of the student or student's family; d. A personal identifier, such as the student's social security number, student number, or biometric record; e. Other indirect identifiers, such as the student's date of birth, place of birth, and Mother's Maiden Name; Examples of staff APPR PII: a. Teacher Id, Social Security Number, Employee Number, Biometric Record b. Name, Mother's Maiden Name, Parent's Name c. Birthdate, Place of Birth, Address d. Gender, Race, Salary ☐ IF YOUR ORGANIZATION/SOFTWARE DOES NOT COLLECT PII, CHECK THIS BOX AND SKIP TO THE BOTTOM, SIGN AND SUBMIT. If you collect the PII information above, please complete the remainder of this form.
Description of the purpose(s) for which Contractor will receive/access PII	Please refer to Renaissance Terms of Service and License Agreement, Exhibit D Data Protection Addendum
Type of PII that Contractor will receive/access	Check all that apply: ☒ Student PII ☐ APPR PII



Contract Term	Contract Start Date <u>11/01/2026</u> Contract End Date <u>10/31/2027</u>
Subcontractor Written Agreement Requirement	Contractor will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Contract. (check applicable option) ☐ Contractor will not utilize subcontractors. ☒ Contractor will utilize subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Contractor shall: • Securely transfer data to EA, or a successor contractor at the EA's option and written discretion, in a format agreed to by the parties. • Securely delete and destroy data.
Challenges to Data Accuracy	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If a correction to data is deemed necessary, the EA will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA's written request.
Secure Storage and Data Security	Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply) ☒ Using a cloud or infrastructure owned and hosted by a third party. ☐ Using Contractor owned and hosted solution ☐ Other: Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data: Please refer to the attached Information Security Overview
Encryption	Data will be encrypted while in motion and at rest.

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Educational Agency (EA) is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan, pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. For every contract, the Contractor must complete the following or provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York state. **While this plan is not required to be posted to the EA's website, contractors should nevertheless ensure that they do not include information that could compromise the security of their data and data systems.**

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	Please refer to attached Information Security Overview.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	Please refer to attached Information Security Overview.
3	Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.	Please refer to attached Information Security Overview.
4	Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.	Please refer to attached Information Security Overview.
5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the EA.	Please refer to attached Information Security Overview.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Please refer to Renaissance Terms of Service and License Agreement Exhibit D Data Protection Addendum
7	Describe your secure destruction practices and how certification will be provided to the EA.	Please refer to Renaissance Terms of Service and License Agreement Exhibit D Data Protection Addendum
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	Please refer to Renaissance Terms of Service and License Agreement Exhibit D Data Protection Addendum
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1	Please refer to attached Information Security Overview.

Additional Information (More information can be provided at the bottom 2 pages):



Western Suffolk BOCES Education Law §2-d Bill of Rights for Data Privacy and Security

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketing purpose. PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.
2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency. This right may not apply to Parents of an Eligible Student.
3. State and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student's identifiable information.
4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.
5. A complete list of all student data elements collected by NYSED is available at www.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.
6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to: dpo@wsboces.org. (ii) Complaints may also be submitted to the NYS Education Department at www.nysed.gov/data-privacy-security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to privacy@nysed.gov; or by telephone at 518-474-0937.
7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.
8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.
9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

CONTRACTOR	
[Signature]	
[Printed Name]	Ted Wolf
[Title]	CFO
Date:	10/08/2026

Additional Information:

Information Security Overview

Welcome educators! As a leading provider of technology products to K–12 schools worldwide, information security is critically important to Renaissance's business. Every day, millions of students, teachers, and administrators depend upon our commitment to protect their data. We take this commitment seriously. This Information Security Overview describes the ways in which we protect your data. Renaissance may update or modify these security measures from time to time provided that such updates and modifications do not materially decrease the overall security of the relevant personal data. If you are interested in learning more about how we handle the privacy of your data (data use, collection, disclosure, and deletion) please visit our Privacy Hub for more information. You may also access our Trust Center to view our SOC 2 Type 2 report and other details about our Privacy Program controls.

Technical Controls Data Storage & Hosting Cloud-Hosted Products: Renaissance products are designed around the core pillars of confidentiality, integrity, and availability. Renaissance products are developed, tested, and deployed in Amazon Web Services (AWS) across several geographically and logically separated locations. AWS complies with an array of industry recognized standards including ISO 27001 and SOC 2. Please visit AWS Global Infrastructure for more information.

Renaissance Data Center: The Renaissance Data Center (RDC) hosts a subset of ancillary systems and data processing activities supporting Renaissance Growth Platform customers. The RDC is located in Wisconsin, USA. Systems processing data run on dedicated servers, network infrastructure, and data stores.

Encryption - Data encryption is an important component of the protection of sensitive data. Renaissance's information security team reviews and updates encryption controls based on the latest standards and guidelines published by Open Web Application Security Project (OWASP) and National Institute of Standards and Technology (NIST). • In transit: Renaissance requires encryption over public connections, using Transport Layer Security (TLS), commonly known as SSL, using industry-standard protocols, ciphers, algorithms, and key sizes. The current standard is TLS 1.2 or better. • At rest: Renaissance requires encryption using industry standard Federal Information Processing Standards (FIPS) approved encryption algorithms. The current standard is AES 256 or better.

Credentials and Access Controls - In-Product Controls: Each school or district has a universally unique identifier within Renaissance products and all data stored and processed in Renaissance applications is associated with the customer identifier. 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. Our products integrate with several Student Information Systems for automated rostering and Single-Sign-On (SSO) providers for tighter identity and authentication controls. **Renaissance Corporate Controls:** Renaissance maintains a role-based access control program built around the principles of least privilege, least functionality, and the implementation of need-to-know. Renaissance employee and contractor accounts are provisioned with a role that provides access based on their job requirements. All accounts require multi-factor authentication and have strong password requirements. Access to Renaissance corporate systems and data requires the use of Renaissance managed devices.

Application Security - Renaissance takes several measures to build products and solutions that are designed to preserve the confidentiality, integrity, and availability of the data entrusted to us. We physically and logically segment our environments to control the movement of data. We establish and enforce baseline configuration and system hardening standards that address secure practices for development, acquisition, configuration, patching, and maintenance. We implement well documented change management processes that require the use of Infrastructure as Code and automated product deployment pipelines, where changes are first developed in a development environment, promoted to a testing or staging environment for quality and security checks, and eventually promoted to production environments for use by customers.

Threat and Vulnerability Management

The Renaissance Threat and Vulnerability Management Program integrates application security testing, vulnerability scanning, and threat modeling with an automated remediation workflow. We implement vulnerability scanners which actively and passively scan assets in both the corporate and product environments. We have also deployed a cloud security platform to scan for vulnerabilities and assess threats in our cloud platform and infrastructure. Our processes assess product configuration for compliance with industry standards and best practices.

We also implement Dynamic Application Security Testing (DAST), utilizing both unauthenticated and authenticated testing schemes based on OWASP standards to discover run-time vulnerabilities in our applications. The DAST process, which is an integral piece of our software development cycle, tests our software for exploitable weaknesses and vulnerabilities before it is deployed to the production environment. The DAST process also plugs into the Threat and Vulnerability Management remediation workflow.

Penetration Testing

Renaissance engages with a third party to conduct penetration tests on each application and its underlying infrastructure annually. Penetration test results are used to validate the security controls we've implemented. All penetration test findings are assessed and remediated through our Threat and Vulnerability Management processes. Fixes are deployed through our product development pipelines.

Endpoint Security

Endpoint detection and response (EDR, also referred to as anti-virus) tooling is installed on Renaissance systems. In the product environments, much of Renaissance's product infrastructure is built on AWS managed services and serverless technology, which provides additional malware detection capability. EDR and our cloud service provider provided malware and intrusion detection systems are integrated into a Managed Detection and Response (MDR) solution for analysis and automated response activities.

Network and Infrastructure Security

Renaissance implements layered network and infrastructure security controls to protect customers' data. We deploy next-generation firewalls, segmented network designs, and segmented cloud infrastructure account designs to control the flow of traffic. We also utilize intrusion detection and prevention systems. Employee and contractor access to Renaissance systems requires the use of managed hardware that implements conditional access controls. Employees and contractors remotely access Renaissance systems using a VPN and Secure Access Service Edge (SASE) solution that utilizes identity-based access and next-generation firewalling.

Logging, Monitoring, and Alerting

Renaissance collects and analyzes an array of log data including system logs, system security configuration logs, access control logs, system process analysis, network traffic analysis, and network bandwidth consumption. Log and activity data is centralized into our MDR, which then correlates and analyzes event data. When anomalous activity or threats are detected by the MDR, automated alerts are sent to our team of responders. We monitor our MDR and our operational systems 24 hours a day, 7 days a week, and any suspicious or anomalous activity is promptly investigated. Business Continuity & Disaster Recovery Renaissance maintains and tests Business Continuity and Disaster Recovery plans to protect your data. Backups are taken at least every 24 hours and are protected using segmentation and vaulting technologies. Additionally, services are deployed into scalable groups and are load balanced across compute and storage services running in geographically diverse availability zones to provide high availability and reduce the risk of service outage. Renaissance also manages much of its cloud infrastructure as code, which facilitates quick recovery or rollback in case of outage, and better transparency into changes in infrastructure over time.

Physical Controls Cloud-Hosted Products: - Renaissance cloud products are hosted on AWS, a durable technology platform that aligns to an array of industry-recognized security and availability standards. For more information about AWS, please visit <https://aws.amazon.com/about-aws/global-infrastructure/>. Renaissance Data Center: The Renaissance Data Center, which hosts a subset of ancillary systems and data processing activities supporting Renaissance Growth Platform customers, is located at Renaissance's corporate headquarters in Wisconsin.

Entry into Renaissance properties is controlled via employee magnetic key entry. Only Cloud Operations and Network Services personnel who are responsible for management of data center infrastructure are allowed unescorted access to the Renaissance data center. Physical access to the data center is controlled through a proximity card system and a motion-based detection system. All visitors to the data center, as well as their internal employee escorts, must sign an access log. We also monitor log files, review access logs, track system usage, and monitor network bandwidth consumption. The environmental conditions within the data center are monitored and maintained at a consistent temperature and humidity range. Electrical power is filtered and controlled by dual uninterruptible power systems. Backup power is provided by an automatic-start generator. Waterless fire protection and an early-warning water systems are also installed and monitored.

Administrative Controls Governance and Risk Management - Renaissance maintains a comprehensive information security program built around the NIST Cybersecurity Framework (CSF).

We implement NIST Special Publication 800-53 controls associated with each of the CSF functions. We also assess our Information Security and Privacy programs against the Center for Internet Security (CIS) Top 18 Controls and annually complete a SOC 2 Type 2 examination of controls. See Compliance below for more information about our SOC 2 Type 2 report.

Cybersecurity Risk Committee: The Renaissance Cybersecurity Risk Committee is charged with identifying, tracking, and managing cybersecurity risks. The committee communicates with executive leadership and the board of directors to keep them informed of key cyber and business level risks facing Renaissance. The Committee is also charged with evaluating Renaissance information security and privacy policies, procedures, and operations along with Renaissance's products, product development, and product deployment systems to identify potential areas of vulnerability and risk. These evaluations are used to develop policy, practices, and priorities to manage risk to an acceptable level.

Incident Response and Incident Reporting - Renaissance maintains an Incident Response Plan and has a standing Incident Response Team. Our incident response plan establishes roles and responsibilities, incident declaration, incident assessment, as well as each of the response phases to include identification, containment, eradication, recovery, reporting, and lessons learned. The Incident Response Team monitors our detection and response systems 24 hours a day, 7 days a week. Suspicious and anomalous activity is promptly investigated. The Incident Response Team also performs Tabletop Exercises at least twice annually. Tabletop Exercise results are used to further refine the Incident Response Plan, policy, and risk management practices. We encourage district representatives with any questions or concerns regarding privacy, security, or related issues to contact our Chief Information Security Officer via e-mail at infosecurity@renaissance.com.

Security Education, Training & Awareness - Renaissance employees and contractors are required to complete Privacy and Information Security training on an annual basis. Renaissance regularly communicates information about the current cybersecurity threat landscape to all employees and contractors. Additionally, Renaissance conducts an anti-phishing and social engineering awareness and training program. Supplemental training events, such as International Privacy Week and Cybersecurity Awareness Month, are also major elements of the training program.

Compliance Audits: Renaissance's enterprise Information Security & Compliance Program completes the SOC 2 Type 2 examination of controls on an annual basis. The examination is formally known as a Type 2 Independent Service Auditor's Report on Controls Relevant to Security and Privacy, and reports on Renaissance's systems and the suitability of the design, implementation, and reporting of our information security and privacy controls. Our SOC 2 Type 2 is scoped to specific products and services. For more information on our audit process, including which products are included in our SOC 2 Type 2 report, please contact infosecurity@renaissance.com or visit our Trust Center. Employees: All Renaissance employees and contractors have a duty to safeguard the data entrusted to them. Additionally, employees and contractors are required to read, sign, and agree to abide by Renaissance's Information Security and Information Technology policies. Background checks are conducted as part of the onboarding process for employees and contractors to the extent permitted by law. Vendors/Sub-processors that Support Our Products: Renaissance maintains a vendor compliance program. Vendors' security and privacy practices are reviewed and analyzed. Additionally, Renaissance

Additional Information:

enters into written contracts with each vendor/sub-processor containing terms that offer similar levels of data protection obligations and protection for customer personally identifiable information as identified in our Data Protection Addendum with customers. Our vendors/sub-processors are documented here: Sub-Processors.

The Renaissance Shared Responsibility Model Effective security and compliance are a shared responsibility between Renaissance and our customers. As a SaaS provider, Renaissance is committed to providing a secure platform to serve our customers' needs. As part of our service, we help relieve the burden of planning, deploying, and maintaining our software and its supporting infrastructure. Renaissance customers assume the responsibility to securely configure and use our products. For Renaissance customers to rely on the information processed by our products, customers are expected to evaluate and implement appropriate security controls in their IT systems. Below is an overview of security and compliance responsibilities.

EXHIBIT D

Data Protection Addendum 1.0 United States. With respect to Authorized Users in the United States, the following provisions shall apply: 1.1 Definitions As used in this Data Protection Addendum, Capitalized words have the meaning set forth in Exhibit A of the Terms of Service or as otherwise expressly defined in this Data Protection Addendum. The following terms have the meanings set forth below for purposes of this Data Protection Addendum. "Data Protection Legislation" means applicable federal, state, local, and municipal laws and regulations in the United States that relate to the privacy, data protection or data security of Customer Personally Identifiable Information, including but not limited to, and to the extent applicable, the Children's Online Privacy Protection Act, 15 U.S.C. § 6501, et seq., and its implementing regulations, 16 C.F.R. Part 312 (together, "COPPA") and the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g, and its implementing regulations, 34 C.F.R. Part 99 (together, "FERPA"). "Personally Identifiable Information" or "PII" means information about an Authorized User that can be used on its own or with other information to identify, contact, or locate a single individual that is provided to Renaissance in connection with providing the Products to the Customer including, but not limited to, the following - Any information that can be used to identify an individual, such as full name and date of birth; - Any other information that is linked to an individual such as educational information. For the avoidance of doubt, PII is a subset of Customer Data.

"Process, Processes, Processing" shall have the same meaning as set out in the applicable Data Protection Legislation or if no such meaning or concept exists, it shall be the means by which Renaissance collects, uses, stores, discloses, or transfers Customer PII. 1.2 Compliance with Laws. Each Party shall comply with all Data Protection Legislation applicable to it in its respective Processing of Customer PII under the Agreement. 1.3 Notices and Consents. Customer shall provide all notices and obtain all such consents required under applicable Data Protection Legislation from the Authorized Users (or such Authorized User's parent or guardian, as applicable) (a) to allow Renaissance to Process the Customer PII and as otherwise described in the Agreement and (b) for Renaissance to Process the Customer PII as described herein and in the Notice of Renaissance's Practices Relating to Children's Online Privacy located here (collectively, the "Notices and Consents"). Customer represents and warrants that it has obtained and will maintain the Notices and Consents for all Authorized Users through the entire term of the Agreement. 1.4 Details of Processing. Renaissance's Notice of Renaissance's Practices Relating to Children's Online Privacy located here sets out certain information regarding Renaissance's Processing of Customer PII of children under 13. For the purposes of this DPA, the Processing activities described in Renaissance's Notice of Renaissance's Practices Relating to Children's Online Privacy also apply to Customer PII from Authorized Users of all ages. Customer acknowledges and agrees that Renaissance's Notice of Renaissance's Practices Relating to Children's Online Privacy, including the Categories of Data Collected by Products available here is subject to change from time to time to remain current Renaissance will not make material changes to the Notice of Renaissance's Practices Relating to Children's Online Privacy without prior notice to Customer. 1.5 Renaissance Obligations. a. Renaissance shall implement, maintain, and use reasonable technical and organizational measures that are designed to preserve the confidentiality and availability of all Customer PII Processed by Renaissance via the Products. Renaissance's technical and organizational measures, as set forth in Renaissance's Information Security Overview, and other product specific Security Overviews, are available in the Renaissance Trust Center. Customer has reviewed such measures and agrees that the measures are appropriate taking into account the state of the art, the costs of implementation, nature, scope, context and purposes of processing Customer PII hereunder. b. Renaissance shall take reasonable steps to ensure the reliability and integrity of any employees who have access to the Customer PII and ensure that employees are under a duty of confidentiality with respect to their Processing of the Customer PII. c. Renaissance engages certain third-party entities to Process the Customer Data on Renaissance's behalf ("Subprocessors"). Renaissance shall enter into a written contract with each Sub-processor containing terms that offer substantially similar levels of data protection obligations and protection for Customer PII as those set out in this Section. Renaissance shall be liable for all acts and omissions of any Subprocessor to the extent Renaissance would be if they were Renaissance's acts or omissions. Customer consents to Renaissance engaging the Subprocessors for the purposes set forth in the Agreement. Customer acknowledges and agrees that the list of Subprocessors available here may be updated from time to time. Renaissance shall make reasonable effort to inform Customer of any changes to the Sub-processors by posting updates on its privacy hub available here. d. If Renaissance becomes aware of a confirmed breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to the Customer PII (a "Security Incident"), Renaissance shall inform Customer, within a reasonable amount of time, taking into account the timescales required by Data Protection Legislation, with respect to the Security Incident Renaissance will provide reasonable information, cooperation, and updates of material developments to enable Customer to fulfill any data breach reporting obligations it may have under Data Protection Legislation.

However, Renaissance's provision of information and cooperation shall be at Customer's cost and expense to the extent any Security Incidents were caused by Customer or its Authorized Users. Renaissance may take such other measures as it deems appropriate to mitigate the effects of the Security Incident. 1.6 Data Subject Inquiries. Customer shall be solely responsible for responding to and fulfilling any inquiries from Authorized Users and other data subjects (collectively, "Data Subjects") regarding their PII in connection with the Processing under this Agreement, including any requests to exercise their rights under applicable Data Protection Legislation, and Customer shall handle all Data Subject's inquiries in accordance with applicable Data Protection Legislation. Customer understands that Renaissance is not required to take any action in response to any requests from Data Subjects except to notify such Data Subjects to contact Customer. Authorized Users may review, obtain a copy of, and amend their own PII by contacting the Customer and following the Customer's procedures for amending PII. To the extent the Customer cannot obtain a copy of, delete, or amend the Customer PII directly within the Product, the Customer may contact Renaissance and Renaissance will provide a copy of, delete, or amend such Data Subject's PII in accordance with Customer's instructions. To the extent Customer is unable to directly service the Data Subject's request via functionality within the Products, and to the extent legally permitted, Customer shall be responsible for reasonable costs arising out of Renaissance's provision of assistance with Customer's Data Subject request Customer shall indemnify, defend, and hold harmless Renaissance and its affiliates, subsidiaries, successors and assigns (and the officers, directors, employees, sublicensees, customers, and agents of Renaissance and its affiliates, subsidiaries, successors, and assigns), from and against any and all losses, demands, liabilities, damages, fines, settlements, expenses, and costs (including without limitation reasonable attorneys' fees and costs), arising from, in connection with, Renaissance complying with Customer's instructions under this Agreement. 1.7 Authorized Disclosure of Customer PII. a. At the request of Customer, Customer acknowledges and agrees that Renaissance may provide Customer PII, to Third-Party Services or other entities to whom Customer requests Renaissance to provide Customer PII (e.g., State Board of Education). Customer shall make such a request to disclose Customer PII either (i) in writing; or (ii) via the Administrator Account (to the extent the functionality exists within the Product) by enabling the data sharing feature from within the Products (each an "Authorization"). Customer acknowledges and agrees that each Authorization will result in Customer electing, in its sole discretion, to transfer the Customer PII to the recipients that Customer selects ("Third-Party Services Recipients").

b. Customer warrants that an individual assigned to the Administrator Account shall be an individual or individuals elected by Customer to have sufficient authority to authorize the transfer of Customer PII to the Third-Party Services Recipients on behalf of the Customer. c. Customer acknowledges that Customer Data may contain PII and may be subject to Data Protection Legislation. Customer will hold Renaissance harmless, and not liable in any way for disclosure of PII to the Third-Party Services Recipients under the terms of the Agreement. d. Renaissance makes no warranty (a) that the use of the Customer PII by the Recipient is valid and in compliance with all applicable Data Protection Legislation and Customer's organization's policies or that Customer PII will remain secure upon transfer to the Recipient and disclaims any responsibility for the transfer. Customer acknowledges that the Customer Data will be provided on as "as is", "as available" basis. 1.8 Data Retention. Customer PII will be deleted within a reasonable amount of time after the data is no longer needed for the purpose for which it was collected, except that Renaissance may retain Customer PII as required by applicable

State Specific Privacy Addendum, law, regulation, court order, or rules applicable to the safeguarding of evidence pending litigation, or as agreed by Customer. 1.9 Renaissance Data. Customer acknowledges and agrees that Renaissance may create Renaissance Data. In generating Renaissance Data, Renaissance shall (a) take reasonable measures to ensure that such information cannot be associated with an Authorized User or a "consumer" or "household" (as defined in Data Protection Legislation), (b) publicly commit to maintain and use the information in deidentified form, and (c) not attempt to reidentify the information, except as permitted under Data Protection Legislation. 1.10 Education Records. As applicable, to the extent Renaissance has access to "Education Records" and "Personally Identifiable Information" (as those terms are defined in FERPA in connection with its provision of the Products) (a) Customer agrees that Renaissance has met the criteria for being a "School Official" with "Legitimate Educational Interests" (as those terms are used in FERPA) in such Education Records and Personally Identifiable Information; and (b) Renaissance agrees that such Education Records and Personally Identifiable Information will be used only for authorized purposes under the Agreement, and it will not redisclose such Education Records or Personally Identifiable Information except with Authorization from Customer and where such redisclosure is otherwise permitted under FERPA.

1.11 Personal Information Collected from Children. To the extent Renaissance collects Personal Information from a child under 13 in connection with its provision of the Products, (a) Renaissance agrees to limit its use of such Personal Information to the purposes authorized by Customer under the Agreement, and (b) Customer consents on behalf of parents or legal guardians to the collection, use, and disclosure of such Personal Information with respect to use of the Products as described in Renaissance's Notice of Renaissance's Practices Relating to Children's Online Privacy located here. 1.12 State Specific Privacy Addenda. If applicable, the parties agree to the State Specific Data Protection Addenda for the applicable state(s).

1.13 Updates to this DPA. Notwithstanding anything to the contrary in the Agreement, Renaissance reserves the right to modify this DPA from time to time in its sole discretion and without Customer's prior consent ("Updated DPA"); provided, where required by applicable law, Renaissance shall obtain Customer's consent to the Updated DPA. Customer agrees that any Updated DPA will be effective immediately upon Renaissance posting such Updated DPA on the privacy hub, unless Renaissance is required by applicable law to obtain Customer's consent, in which case, such Updated DPA will be effective immediately upon the provision of such consent. Renaissance will also endeavor to notify Customer of any material revision to this DPA at least 10 days prior to such revision coming into effect, using Customer's email address as set forth in the Quote.

