

## **New York**

This Student Data Privacy Agreement (“**DPA**”) is entered into on the date of full execution (the “**Effective Date**”) and is entered into by and between: Washington-Saratoga-Warren-Hamilton-Essex BOCES (the “**Local Education Agency**” or “**LEA**” or “**New York Original LEA**”) and ProQuest LLC (the “**Provider**”).

**WHEREAS**, the Provider is providing educational or digital services to LEA.

**WHEREAS**, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act (“**FERPA**”) at 20 U.S.C. § 1232g (34 CFR Part 99); the Children’s Online Privacy Protection Act (“**COPPA**”) at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations and

**WHEREAS**, the documents and data transferred from LEAs and created by the Provider’s Services are also subject to several state laws in New York. Specifically, those are New York Education Law § 2-d; and the Regulations of the Commissioner of Education at 8 NYCRR Part 121; and

**WHEREAS**, the Parties wish to enter into these additional terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

**NOW THEREFORE**, for good and valuable consideration, the parties agree as follows:

1. Provider agrees to offer the LEA all the same terms and conditions found in the **MA-ME-NH-RI-VT-NDPA, Standard Version 1.0** Data Privacy Agreement between the Provider and **Maine School Administrative District 51** (Originating LEA”) which is dated **9/14/23** (“Originating DPA”). The terms and conditions of the Originating DPA are thus incorporated herein.
2. Provider additionally agrees to the following additional terms outlined in the attached Exhibit “G” for New York, which will control in the event of a conflict between the DPA and the Originating DPA.
3. Provider may, by signing the attached form of “General Offer of Privacy Terms” be bound by the terms of the General Offer of Privacy Terms to any other LEA who signs the acceptance on said Offer. The form is limited by the terms and conditions described therein.
4. **Notices**. All notices or other communication required or permitted to be given pursuant to the Originating DPA may be given for the LEA via e-mail transmission, or first-class mail, sent to the designated representatives below.

The designated representative for the Provider for this DPA is:

Name: Karen Smith

Title: Data Protection Officer, Senior VP, Chief Compliance and Privacy Officer

Address: 789 E. Eisenhower Pkwy, Ann Arbor, MI 48108

Phone: 855-CLV-5858

Email: Karen.Smith@clarivate.com

The designated representative for the LEA for this DPA is:

Sarah McCann, Lead Coordinator for Data Privacy

10 LaCrosse Street, Suite 6, Hudson Falls, NY 12839

SMccann@wswheboces.org 518-581-3514

### ProQuest LLC

By: 

Date: November 21, 2025

Printed Name: Tim McGee

Title/Position: VP, Sales Operations

### Washington-Saratoga-Warren-Hamilton-Essex BOCES

  
Anthony Muller Dec 2, 2025 09:59:51 EST

Date: Dec 2, 2025

Printed Name: Anthony Muller

Title/Position: Interim Senior Executive Officer

## **Exhibit “G”**

### **New York**

1. All employees of the Provider who will have direct contact with students shall pass criminal
2. background checks.
3. Student Data will be used by Provider exclusively to provide the Services identified in Exhibit A to the DPA.
4. Provider agrees to maintain the confidentiality and security of Student Data in accordance with LEA’s Data Security and Privacy Policy. The LEA’s Data Security Policy is attached hereto as Exhibit J. Each Subscribing LEA will provide its Data Security Policy to the Provider upon execution of Exhibit “E”. Provider shall use industry standard security measures including encryption protocols that comply with New York law and regulations to preserve and protect Student Data and APPR Data. Provider must Encrypt Student Data and APPR Data at rest and in transit in accordance with applicable New York laws and regulations.
5. Provider represents that their Data Privacy and Security Plan can be found at the URL link listed in Exhibit K and is incorporated into this DPA. Provider warrants that its Data Security and Privacy Plan, at a minimum: (a) implements all applicable state, federal and local data privacy and security requirements; (b) has operational technical safeguards and controls in place to protect PII that it will receive under the service agreement; (c) complies with the LEA’s parents bill of rights for data privacy and security; (d) requires training of all providers’ employees, assignees and subprocessors who have Access to student data or APPR data; (e) ensures subprocessors are required to protect PII received under this service agreement; (f) specifies how data security and privacy incidents that implicate PII will be managed and ensuring prompt notification to the LEA, and (g) addresses Student Data return, deletion and destruction.
6. In addition to the requirements described in Paragraph 3 above, the Provider's Data Security and Privacy Plan shall be deemed to incorporate the LEA's Parents Bill of Rights for Data Security and Privacy, as found at the URL link identified in Exhibit J. The Subscribing LEA will provide its Parents Bill of Rights for Data Security and Privacy to the Provider upon execution of Exhibit “E”.
7. All references in the DPA to “Student Data” shall be amended to include and state, “Student Data and APPR Data.”
8. To amend Article II, Section 5 to add: Provider shall ensure that its subprocessors agree that they do not have any property, licensing or ownership rights or claims to Student Data or APPR data and that they will comply with the LEA’s Data Privacy and Security Policy. Provider shall examine the data privacy and security measures of its Subprocessors. If at any point a Subprocessor fails to materially comply with the requirements of this DPA, Provider shall: (i) notify LEA, (ii) as applicable, remove such Subprocessor’s Access to Student Data and APPR Data; and (iii) as applicable, retrieve all Student Data and APPR Data received or stored by such Subprocessor and/or ensure that Student Data and APPR

Data has been securely deleted or securely destroyed in accordance with this DPA. In the event there is an incident in which Student Data and APPR Data held, possessed, or stored by the Subprocessor is compromised, or unlawfully Accessed or disclosed, Provider shall follow the Data Breach reporting requirements set forth in the DPA.

9. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
10. To amend Article IV, Section 3 to add: Provider shall ensure that all its employees and subprocessors who have Access to or will receive Student Data and APPR Data will be trained on the federal and state laws governing confidentiality of such Student Data and APPR Data prior to receipt. Access to or Disclosure of Student Data and APPR Data shall only be provided to Provider’s employees and subprocessors who need to know the Student Data and APPR Data to provide the services and such Access and/or Disclosure of Student Data and APPR Data shall be limited to the extent necessary to provide such services.
11. To replace Article IV, Section 6 (Disposition of Data) with the following: Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within ninety (90) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Provider is prohibited from retaining disclosed Student Data or continuing to Access Student Data beyond the term of the Service Agreement unless such retention is expressly authorized for a prescribed period by the Service Agreement, necessary for purposes of facilitating the transfer of disclosed Student Data to the LEA, or expressly required by law. The confidentiality and data security obligations of Provider under this DPA shall survive any termination of this contract to which this DPA is attached but shall terminate upon Provider’s certifying that it and its subprocessors, as applicable: (a) no longer have the ability to Access any Student Data provided to Provider pursuant to the Service Agreement and/or (b) have destroyed all Student Data and APPR Data provided to Provider pursuant to this DPA. The Provider agrees that the timelines for disposition of data will be modified by any Assurance of Discontinuation, which will control in the case of a conflict.

Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all student data after providing the LEA with ninety (90) days prior notice.

The duty to dispose of student data shall not extend to Student Data that had been de-identified or placed in a separate student account pursuant to section II 3. The LEA may employ a “**Directive for Disposition of Data**” form, a copy of which is attached hereto as **Exhibit “D”**, or, with reasonable notice to the Provider, other form of its choosing. No further written request or notice is required on the part of either party prior to the disposition of Student Data described in “**Exhibit D**”.

12. To amend Article IV, Section 7 to add: 'Notwithstanding the foregoing, Provider is prohibited from using Student Data or APPR data for any Commercial or Marketing Purpose as defined herein. And add after (iii) account holder, "which term shall not include students."
13. To replace Article V, Section 1 (Data Storage) to state: Student Data and APPR Data shall be stored within the United States and Canada only. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.
14. To replace Article V, Section 2 (Audits) to state: No more than once a year or following an unauthorized Access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA or its designee(s) to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA. The Provider will cooperate reasonably with the LEA or its designee(s) and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable Access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA.

Upon request by the New York State Education Department's Chief Privacy Officer (NYSED CPO), Provider shall provide the NYSED CPO with copies of its policies and related procedures that pertain to the protection of information. In addition, the NYSED CPO may require Provider to undergo an audit of its privacy and security safeguards, measures, and controls as they pertain to alignment with the requirements of New York State laws and regulations, and alignment with the NIST Cybersecurity Framework. Any audit required by the NYSED CPO must be performed by an independent third party at Provider's expense and the audit report must be provided to the NYSED CPO. In lieu of being subject to a required audit, Provider may provide the NYSED CPO with an industry standard independent audit report of Provider's privacy and security practices that was issued no more than twelve months before the date that the NYSED CPO informed Provider that it required Provider to undergo an audit. Failure to reasonably cooperate with any of the requirements in this provision shall be deemed a material breach of the DPA.

To amend the third sentence of Article V. Section 3 (Data Security) to read: The Provider shall implement security practices that are in alignment with the NIST Cybersecurity Framework v1.1 or any update to this Framework that is adopted by the New York State Department of Education.

15. To replace Article V. Section 4 (Data Breach) to state: In the event of a Breach as defined in 8 NYCRR Part 121.1 Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident or no more than 7 calendar days, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:
  - (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:

- i. The name and contact information of the reporting LEA subject to this section.
  - ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
  - iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
  - iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and
  - v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided; and
  - vi. The number of records affected, if known; and
  - vii. A description of the investigation undertaken so far; and
  - viii. The name of a point of contact for Provider.
- (2) Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
- (3) Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a summary of said written incident response plan.
- (4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians. Where a Breach of Student Data and/or APPR Data occurs that is attributable to Provider and/or its Subprocessors, Provider shall pay for or promptly reimburse LEA for the full cost of notification to Parents, Eligible Students, teachers, and/or principals.
- (5) In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.
- (6) Provider and its subprocessors will cooperate with the LEA, the NYSED Chief Privacy Officer and law enforcement where necessary, in any investigations into a Breach. Any costs incidental to the required cooperation or participation of the Provider will be the sole responsibility of the Provider if such Breach is attributable to Provider or its subprocessors.

16. To amend the definitions in Exhibit "C" as follows:

- "Subprocessor" is equivalent to subcontractor. It is a third party who the provider uses for data collection, analytics, storage, or other service to allow Provider to operate and/or improve its service, and who has access to Student Data.
- "Provider" is also known as third party contractor. It any person or entity, other than an educational agency, that receives student data or teacher or principal data from an educational agency pursuant to a contract or other written agreement for purposes of providing services to

such educational agency, including but not limited to data management or storage services, conducting studies for or on behalf of such educational agency, or audit or evaluation of publicly funded programs. Such term shall include an educational partnership organization that receives student and/or teacher or principal data from a school district to carry out its responsibilities and is not an educational agency and a not-for-profit corporation or other non-profit organization, other than an educational agency.

17. To add to Exhibit "C" the following definitions:

- **Access:** The ability to view or otherwise obtain, but not copy or save, Student Data and/or APPR Data arising from the on-site use of an information system or from a personal meeting.
- **APPR Data:** Personally Identifiable Information from the records of an Educational Agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§ 3012-c and 3012-d
- **Commercial or Marketing Purpose:** In accordance with § 121.1(c) of the regulations of the New York Commissioner of Education, the Disclosure, sale, or use of Student or APPR Data for the purpose of directly or indirectly receiving remuneration, including the Disclosure, sale, or use of Student Data or APPR Data for advertising purposes, or the Disclosure, sale, or use of Student Data to develop, improve, or market products or services to Students.
- **Disclose or Disclosure:** The intentional or unintentional communication, release, or transfer of Student Data and/or APPR Data by any means, including oral, written, or electronic.
- **Encrypt or Encryption:** As defined in the Health Insurance Portability and Accountability Act of 1996 Security Rule at 45 CFR § 164.304, encrypt means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or indecipherable form in which there is a low probability of assigning meaning without use of a confidential process or key.
- **Release:** Shall have the same meaning as Disclose
- **LEA:** As used in this DPA and all Exhibits, the term LEA shall mean the educational agency, as defined in Education Law Section 2-d, that has executed the DPA; if the LEA is a board of cooperative educational services, then the term LEA shall also include Participating School Districts for purposes of the following provisions of the DPA: Article I, Section 2; Article II, Sections 1 and 3; and Sections 1, 2, and 3 of Article III.
- **Participating School District:** As used in Exhibit G and other Exhibits to the DPA, the term Participating School District shall mean a New York State educational agency, as that term is defined in Education Law Section 2-d, that obtains access to the Services through a CoSer agreement with LEA, and shall include LEA if it uses the Services in its own educational or operational programs.

-

## **Exhibit “J”**

### **LEA Documents**

LEA’s Data Security and Privacy Policy, Parents Bill of Rights for Data Security and Privacy, and supplemental information for this service agreement can be accessed at:

[https://sdpc.a4l.org/ny\\_dp\\_bor\\_url.php?districtID=12870](https://sdpc.a4l.org/ny_dp_bor_url.php?districtID=12870)



**Exhibit “K”**

**Provider Security Policy**

Provider’s Data Security and Privacy Plan can be accessed at:

<https://clarivate.com/trust-center/>

---







# ProQuest\_WashingtonSaratoga\_Signed

Final Audit Report

2025-12-02

Created:	2025-12-01
By:	TEC SDPA (mmcgrath@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAAM4ccXbKE-Gh4tiyPhw6vOvGyyM3rg5Uu

## "ProQuest\_WashingtonSaratoga\_Signed" History

-  Document created by TEC SDPA (mmcgrath@tec-coop.org)  
2025-12-01 - 4:11:45 PM GMT
-  Document emailed to tmuller@wswheboces.org for signature  
2025-12-01 - 4:13:29 PM GMT
-  Email viewed by tmuller@wswheboces.org  
2025-12-02 - 2:38:47 PM GMT
-  Signer tmuller@wswheboces.org entered name at signing as Anthony Muller  
2025-12-02 - 2:39:49 PM GMT
-  Document e-signed by Anthony Muller (tmuller@wswheboces.org)  
Signature Date: 2025-12-02 - 2:39:51 PM GMT - Time Source: server
-  Agreement completed.  
2025-12-02 - 2:39:51 PM GMT

**STANDARD STUDENT DATA PRIVACY AGREEMENT**

**MASSACHUSETTS, MAINE, NEW HAMPSHIRE, RHODE ISLAND, AND VERMONT**

**MA-ME-NH-RI-VT-NDPA, Standard Version 1.0**

**Maine School Administrative District 51**

**and**

**ProQuest LLC**

This Student Data Privacy Agreement (“**DPA**”) is entered into on the date of full execution (the “**Effective Date**”) and is entered into by and between: Maine School Administrative District 51, located at 357 Tuttle Road, Cumberland, ME 04021 USA (the “**Local Education Agency**” or “**LEA**”) and ProQuest LLC, located at LC 789 E. Eisenhower Pky, Ann Arbor, MI 48108 (the “**Provider**”).

**WHEREAS**, the Provider is providing educational or digital services to LEA.

**WHEREAS**, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act (“**FERPA**”) at 20 U.S.C. § 1232g (34 CFR Part 99); the Children’s Online Protection Act (“**COPPA**”) at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations and

**WHEREAS**, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.

**NOW THEREFORE**, for good and valuable consideration, LEA and Provider agree as follows:

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.
2. **Special Provisions. Check if Required**
  - ☒ If checked, the Supplemental State Terms and attached hereto as **Exhibit “G”** are hereby incorporated by reference into this DPA in their entirety.
  - ☒ If Checked, the Provider, has signed **Exhibit “E”** to the Standard Clauses, otherwise known as General Offer of Privacy Terms
3. In the event of a conflict between the SDPC Standard Clauses, the State or Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this DPA shall control.
4. This DPA shall stay in effect for three years. Exhibit E will expire 3 years from the date the original DPA was signed.
5. The services to be provided by Provider to LEA pursuant to this DPA are detailed in **Exhibit “A”** (the “**Services**”).
6. **Notices.** All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or first-class mail, sent to the designated representatives below.

**The designated representative for the Provider for this DPA is:**

Name: Anne Marie Schaub Title: Director, Assistant General Counsel

Address: 789 E. Eisenhower Parkway, Ann Arbor, MI 48108

Phone: 1 734 646 9059

Email: annemarie.schaub@clarivate.com

**The designated representative for the LEA for this DPA is:**

Dirk Van Curan, Technology Director  
357 Tuttle Road, Cumberland, ME 04021  
Phone: (207) 829-4800  
dvancuran@msad51.org

**IN WITNESS WHEREOF**, LEA and Provider execute this DPA as of the Effective Date.

**Maine School Administrative District 51**

By: *Dirk Van Curan*  
Dirk Van Curan (Sep 14, 2023 15:09 EDT)

Date: 09/14/2023

Printed Name: Dirk Van Curan

Title/Position: Director of Technology

**ProQuest LLC**

By: *Dawn Branham*

Date: 8/21/23

Printed Name: Dawn Branham

Title/Position: Director, Order Management

## **STANDARD CLAUSES**

Version 1.0

### **ARTICLE I: PURPOSE AND SCOPE**

1. **Purpose of DPA.** The purpose of this DPA is to describe the duties and responsibilities to protect Student Data including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. In performing these services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA, with respect to its use of Student Data.
2. **Student Data to Be Provided.** In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit "B"**.
3. **DPA Definitions.** The definition of terms used in this DPA is found in **Exhibit "C"**. In the event of a conflict, definitions used in this DPA shall prevail over terms used in any other writing, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies etc.

### **ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS**

1. **Student Data Property of LEA.** All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement, shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEA as it pertains to the use of Student Data, notwithstanding the above.
2. **Parent Access.** To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than forty five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA's request for Student Data in a student's records held by the Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.
3. **Separate Account.** If Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student-Generated Content to a separate account created by the student.

4. **Law Enforcement Requests.** Should law enforcement or other government entities (“Requesting Party(ies)”) contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.
5. **Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA.

### ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws.** LEA shall provide Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.
2. **Annual Notification of Rights.** If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its annual notification of rights.
3. **Reasonable Precautions.** LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted Student Data.
4. **Unauthorized Access Notification.** LEA shall notify Provider promptly of any known unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

### ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance.** The Provider shall comply with all applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.
2. **Authorized Use.** The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in Exhibit A or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA.
3. **Provider Employee Obligation.** Provider shall require all of Provider’s employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Student Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.
4. **No Disclosure.** Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non-public information and/or personally identifiable information contained in the Student Data other than as directed or

permitted by the LEA or this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not Sell Student Data to any third party.

5. **De-Identified Data**: Provider agrees not to attempt to re-identify de-identified Student Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; and (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Except for Subprocessors, Provider agrees not to transfer de-identified Student Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to the LEA who has provided prior written consent for such transfer. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which de-identified data is presented.
6. **Disposition of Data**. Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to section II 3. The LEA may employ a "Directive for Disposition of Data" form, a copy of which is attached hereto as **Exhibit "D"**. If the LEA and Provider employ Exhibit "D," no further written request or notice is required on the part of either party prior to the disposition of Student Data described in Exhibit "D."
7. **Advertising Limitations**. Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits

## **ARTICLE V: DATA PROVISIONS**

1. **Data Storage**. Where required by applicable law, Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.
2. **Audits**. No more than once a year, or following unauthorized access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA . The Provider will cooperate reasonably with the LEA and any local, state, or federal



agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA. Failure to reasonably cooperate shall be deemed a material breach of the DPA.

3. **Data Security.** The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The provider shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth in **Exhibit "F"**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit "F"**. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.
4. **Data Breach.** In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:
  - (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:
    - i. The name and contact information of the reporting LEA subject to this section.
    - ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
    - iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
    - iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and
    - v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
  - (2) Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
  - (3) Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a summary of said written incident response plan.

- (4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians.
- (5) In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

## **ARTICLE VI: GENERAL OFFER OF TERMS**

Provider may, by signing the attached form of "General Offer of Privacy Terms" (General Offer, attached hereto as **Exhibit "E"**), be bound by the terms of **Exhibit "E"** to any other LEA who signs the acceptance on said Exhibit. The form is limited by the terms and conditions described therein.

## **ARTICLE VII: MISCELLANEOUS**

1. **Termination.** In the event that either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. Either party may terminate this DPA and any service agreement or contract if the other party breaches any terms of this DPA.
2. **Effect of Termination Survival.** If the Service Agreement is terminated, the Provider shall destroy all of LEA's Student Data pursuant to Article IV, section 6.
3. **Priority of Agreements.** This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between the SDPC Standard Clauses and the Supplemental State Terms, the Supplemental State Terms will control. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.
4. **Entire Agreement.** This DPA and the Service Agreement constitute the entire agreement of the Parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the Parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both Parties. Neither failure nor delay on the part of any Party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.

5. **Severability.** Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the Parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.
6. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE LEA, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY OF THE LEA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.
7. **Successors Bound:** This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business. In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement. The LEA has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.
8. **Authority.** Each party represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof.
9. **Waiver.** No delay or omission by either party to exercise any right hereunder shall be construed as a waiver of any such right and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

## **EXHIBIT "A"**

### **DESCRIPTION OF SERVICES**

ProQuest LLC research solutions, age-appropriate content that covers core curriculum, databases to support classroom instruction, and interactive media. Detailed Schedules A & B are attached and incorporated by reference for the following product/platform/interface configurations

- ProQuest® Platform
- ProQuest® K-12 Guided Research Student Interface (SIRS® and e Library®)
- CultureGrams
- Alexander Street and Alexander Street Video
- History Vault
- ProQuest Ebook Central®
- ProQuest® Research Companion

**EXHIBIT "B"**  
**SCHEDULE OF DATA**

Category of Data	Elements	Check if Used by Your System
Application Technology Meta Data	IP Addresses of users, Use of cookies, etc.	
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	
Assessment	Standardized test scores	
	Observation data	
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications captured (emails, blog entries)	
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, or primary language spoken by student)	
	Other demographic information-Please specify:	
Enrollment	Student school enrollment	
	Student grade level	
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information-Please specify:	
Parent/Guardian Contact Information	Address	
	Email	
	Phone	

Category of Data	Elements	Check if Used by Your System
Parent/Guardian ID	Parent ID number (created to link parents to students)	
Parent/Guardian Name	First and/or Last	
Schedule	Student scheduled courses	
	Teacher names	
Special Indicator	English language learner information	
	Low income status	
	Medical alerts/ health data	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information-Please specify:	
Student Contact Information	Address	
	Email	
	Phone	
Student Identifiers	Local (School district) ID number	
	State ID number	
	Provider/App assigned student ID number	
	Student app username	
	Student app passwords	
Student Name	First and/or Last	
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	
Student work	Student generated content; writing, pictures, etc.	
	Other student work data -Please specify:	
Transcript	Student course grades	
	Student course data	
	Student course grades/ performance scores	

Category of Data	Elements	Check if Used by Your System
	Other transcript data - Please specify:	
Transportation	Student bus assignment	
	Student pick up and/or drop off location	
	Student bus card ID number	
	Other transportation data – Please specify:	
Other	Please list each additional data element used, stored, or collected by your application:	
None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	

## **EXHIBIT "C"**

### **DEFINITIONS**

**De-Identified Data and De-Identification:** Records and information are considered to be de-identified when all personally identifiable information has been removed or obscured, such that the remaining information does not reasonably identify a specific individual, including, but not limited to, any information that, alone or in combination is linkable to a specific student and provided that the educational agency, or other party, has made a reasonable determination that a student's identity is not personally identifiable, taking into account reasonable available information.

**Educational Records:** Educational Records are records, files, documents, and other materials directly related to a student and maintained by the school or local education agency, or by a person acting for such school or local education agency, including but not limited to, records encompassing all the material kept in the student's cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs.

**Metadata:** means information that provides meaning and context to other data being collected; including, but not limited to: date and time records and purpose of creation Metadata that have been stripped of all direct and indirect identifiers are not considered Personally Identifiable Information.

**Operator:** means the operator of an internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used for K–12 school purposes. Any entity that operates an internet website, online service, online application, or mobile application that has entered into a signed, written agreement with an LEA to provide a service to that LEA shall be considered an "operator" for the purposes of this section.

**Originating LEA:** An LEA who originally executes the DPA in its entirety with the Provider.

**Provider:** For purposes of the DPA, the term "Provider" means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Student Data. Within the DPA the term "Provider" includes the term "Third Party" and the term "Operator" as used in applicable state statutes.

**Student Generated Content:** The term "student-generated content" means materials or content created by a student in the services including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of student content.

**School Official:** For the purposes of this DPA and pursuant to 34 CFR § 99.31(b), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of Student Data including Education Records; and (3) Is subject to 34 CFR § 99.33(a) governing the use and re-disclosure of personally identifiable information from Education Records.

**Service Agreement:** Refers to the Contract, Purchase Order or Terms of Service or Terms of Use.



**Student Data:** Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data includes Meta Data. Student Data further includes "personally identifiable information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local laws and regulations. Student Data as specified in Exhibit "B" is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services.

**Subprocessor:** For the purposes of this DPA, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its service, and who has access to Student Data.

**Subscribing LEA:** An LEA that was not party to the original Service Agreement and who accepts the Provider's General Offer of Privacy Terms.

**Targeted Advertising:** means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the operator's Internet web site, online service or mobile application by such student or the retention of such student's online activities or requests over time for the purpose of targeting subsequent advertisements. "Targeted advertising" does not include any advertising to a student on an Internet web site based on the content of the web page or in response to a student's response or request for information or feedback.

**Third Party:** The term "Third Party" means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Education Records and/or Student Data, as that term is used in some state statutes. However, for the purpose of this DPA, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

**EXHIBIT "D"**  
**DIRECTIVE FOR DISPOSITION OF DATA**

**[Insert Name of District or LEA]** Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

\_\_\_\_\_ Disposition is partial. The categories of data to be disposed of are set forth below or are found in an attachment to this Directive:

**[Insert categories of data here]**

\_\_\_\_\_ Disposition is Complete. Disposition extends to all categories of data.

2. Nature of Disposition

\_\_\_\_\_ Disposition shall be by destruction or deletion of data.

\_\_\_\_\_ Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

**[Insert or attach special instructions]**

3. Schedule of Disposition

Data shall be disposed of by the following date:

\_\_\_\_\_ As soon as commercially practicable.

\_\_\_\_\_ By **[Insert Date]**

4. Signature

\_\_\_\_\_  
Authorized Representative of LEA

\_\_\_\_\_  
Date

5. Verification of Disposition of Data

\_\_\_\_\_  
Authorized Representative of Company

\_\_\_\_\_  
Date

**EXHIBIT “F”**  
**DATA SECURITY REQUIREMENTS**

**Adequate Cybersecurity Frameworks**

**2/24/2020**

The Education Security and Privacy Exchange (“Edspex”) works in partnership with the Student Data Privacy Consortium and industry leaders to maintain a list of known and credible cybersecurity frameworks which can protect digital learning ecosystems chosen based on a set of guiding cybersecurity principles\* (“Cybersecurity Frameworks”) that may be utilized by Provider .

**Cybersecurity Frameworks**

	<b>MAINTAINING ORGANIZATION/GROUP</b>	<b>FRAMEWORK(S)</b>
<input type="checkbox"/>	National Institute of Standards and Technology	NIST Cybersecurity Framework Version 1.1
<input type="checkbox"/>	National Institute of Standards and Technology	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
<input checked="" type="checkbox"/>	International Standards Organization	Information technology — Security techniques — Information security management systems (ISO 27000 series)
<input type="checkbox"/>	Secure Controls Framework Council, LLC	Security Controls Framework (SCF)
<input type="checkbox"/>	Center for Internet Security	CIS Critical Security Controls (CSC, CIS Top 20)
<input type="checkbox"/>	Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S))	Cybersecurity Maturity Model Certification (CMMC, ~FAR/DFAR)

Please visit <http://www.edspex.org> for further details about the noted frameworks.

\*Cybersecurity Principles used to choose the Cybersecurity Frameworks are located here

**EXHIBIT “G”**  
**Massachusetts**

**WHEREAS**, the documents and data transferred from LEAs and created by the Provider’s Services are also subject to several state laws in Massachusetts. Specifically, those laws are 603 C.M.R. 23.00, Massachusetts General Law, Chapter 71, Sections 34D to 34H and 603 CMR 28.00; and

**WHEREAS**, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

**WHEREAS**, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Massachusetts;

**NOW THEREFORE**, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Massachusetts does not require data to be stored within the United States.

## **EXHIBIT "G"**

### **Maine**

**WHEREAS**, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Maine. Specifically, those laws are 20-A M.R.S. §6001-6005.; 20-A M.R.S. §951 et. seq., Maine Unified Special Education Regulations, Maine Dep't of Edu. Rule Ch. 101; and

**WHEREAS**, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

**WHEREAS**, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Maine;

**NOW THEREFORE**, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Maine does not require data to be stored within the United States.
4. The Provider may not publish on the Internet or provide for publication on the Internet any Student Data.
5. If the Provider collects student social security numbers, the Provider shall notify the LEA of the purpose the social security number will be used and provide an opportunity not to provide a social security number if the parent and/or student elects.
6. The parties agree that the definition of Student Data in Exhibit "C" includes the name of the student's family members, the student's place of birth, the student's mother's maiden name, results of assessments administered by the State, LEA or teacher, including participating information, course transcript information, including, but not limited to, courses taken and completed, course grades and grade point average, credits earned and degree, diploma, credential attainment or other school exit information, attendance and mobility information between and within LEAs within Maine, student's gender, race and ethnicity, educational program participation information required by state or federal law and email.
7. The parties agree that the definition of Student Data in Exhibit "C" includes information that:
  - a. Is created by a student or the student's parent or provided to an employee or agent of the LEA or a Provider in the course of the student's or parent's use of the Provider's website, service or application for kindergarten to grade 12 school purposes;
  - b. Is created or provided by an employee or agent of the LEA, including information provided to the Provider in the course of the employee's or agent's use of the Provider's website, service or application for kindergarten to grade 12 school purposes; or
  - c. Is gathered by the Provider through the operation of the Provider's website, service or application for kindergarten to grade 12 school purposes.

**EXHIBIT “G”**  
**Rhode Island**

**WHEREAS**, the documents and data transferred from LEAs and created by the Provider’s Services are also subject to several state laws in Rhode Island. Specifically, those laws are R.I.G.L. 16-71-1, et. seq., R.I.G.L. 16-104-1, and R.I.G.L., 11-49.3 et. seq.; and

**WHEREAS**, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

**WHEREAS**, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Rhode Island;

**NOW THEREFORE**, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Rhode Island does not require data to be stored within the United States.
4. The Provider agrees that this DPA serves as its written certification of its compliance with R.I.G.L. 16-104-1.
5. The Provider agrees to implement and maintain a risk-based information security program that contains reasonable security procedures.
6. In the case of a data breach, as a part of the security breach notification outlined in Article V, Section 4(1), the Provider agrees to provide the following additional information:
  - i. Information about what the Provider has done to protect individuals whose information has been breached, including toll free numbers and websites to contact:
    1. The credit reporting agencies
    2. Remediation service providers
    3. The attorney general
  - ii. Advice on steps that the person whose information has been breached may take to protect himself or herself.
  - iii. A clear and concise description of the affected parent, legal guardian, staff member, or eligible student’s ability to file or obtain a police report; how an affected parent, legal guardian, staff member, or eligible student’s requests a security freeze and the necessary information to be provided when requesting the security freeze; and that fees may be required to be paid to the consumer reporting agencies.

## **EXHIBIT “G”**

### **Vermont**

**WHEREAS**, the documents and data transferred from LEAs and created by the Provider’s Services are also subject to several state laws in Vermont. Specifically, those laws are 9 VSA 2443 to 2443f; 16 VSA 1321 to 1324; and

**WHEREAS**, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

**WHEREAS**, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Vermont;

**NOW THEREFORE**, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Vermont does not require data to be stored within the United States.

**EXHIBIT "G"**  
**New Hampshire**

**WHEREAS**, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in New Hampshire. Specifically, those laws are RSA 189:1-e and 189:65-68-a; RSA 186; NH Admin. Code Ed. 300 and NH Admin. Code Ed. 1100; and

**WHEREAS**, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

**WHEREAS**, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for New Hampshire;

**NOW THEREFORE**, for good and valuable consideration, the parties agree as follows:

1. All references in the DPA to "Student Data" shall be amended to state "Student Data and Teacher Data." "Teacher Data" is defined as at least the following:

Social security number.  
Date of birth.  
Personal street address.  
Personal email address.  
Personal telephone number  
Performance evaluations.

Other information that, alone or in combination, is linked or linkable to a specific teacher, paraprofessional, principal, or administrator that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify any with reasonable certainty.

Information requested by a person who the department reasonably believes or knows the identity of the teacher, paraprofessional, principal, or administrator to whom the education record relates.

"Teacher" means teachers, paraprofessionals, principals, school employees, contractors, and other administrators.

2. In order to perform the Services described in the DPA, the LEA shall provide the categories of Teacher Data described in the Schedule of Data, attached hereto as **Exhibit "I"**.
3. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
4. In Article IV, Section 7 amend each reference to "students," to state: "students, teachers,..."
5. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
6. Provider is prohibited from leasing, renting, or trading Student Data or Teacher Data to (a) market or advertise to students, teachers, or families/guardians; (b) inform, influence, or enable marketing, advertising or other commercial efforts by a Provider; (c) develop a profile of a student, teacher, family member/guardian or group, for any commercial purpose other than providing the Service to LEA; or (d) use the Student Data and Teacher Data for the development of commercial products or services, other than as necessary to provide the Service to the LEA. This section does not prohibit Provider from using Student Data and Teacher Data for adaptive learning or customized student learning purposes.



7. The Provider agrees to the following privacy and security standards. Specifically, the Provider agrees to:
- (1) Limit system access to the types of transactions and functions that authorized users, such as students, parents, and LEA are permitted to execute;
  - (2) Limit unsuccessful logon attempts;
  - (3) Employ cryptographic mechanisms to protect the confidentiality of remote access sessions;
  - (4) Authorize wireless access prior to allowing such connections;
  - (5) Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity;
  - (6) Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions;
  - (7) Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles;
  - (8) Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services;
  - (9) Enforce a minimum password complexity and change of characters when new passwords are created;
  - (10) Perform maintenance on organizational systems;
  - (11) Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance;
  - (12) Ensure equipment removed for off-site maintenance is sanitized of any Student Data or Teacher Data in accordance with NIST SP 800-88 Revision 1;
  - (13) Protect (i.e., physically control and securely store) system media containing Student Data or Teacher Data, both paper and digital;
  - (14) Sanitize or destroy system media containing Student Data or Teacher Data in accordance with NIST SP 800-88 Revision 1 before disposal or release for reuse;
  - (15) Control access to media containing Student Data or Teacher Data and maintain accountability for media during transport outside of controlled areas;
  - (16) Periodically assess the security controls in organizational systems to determine if the controls are effective in their application and develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems;

- (17) Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems;
- (18) Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception);
- (19) Protect the confidentiality of Student Data and Teacher Data at rest;
- (20) Identify, report, and correct system flaws in a timely manner;
- (21) Provide protection from malicious code (i.e. Antivirus and Antimalware) at designated locations within organizational systems;
- (22) Monitor system security alerts and advisories and take action in response; and
- (23) Update malicious code protection mechanisms when new releases are available.

Alternatively, the Provider agrees to comply with one of the following standards: (1) NIST SP 800-171 rev 2, Basic and Derived Requirements; (2) NIST SP 800-53 rev 4 or newer, Low Impact Baseline or higher; (3) FedRAMP (Federal Risk and Authorization Management Program); (4) ISO/IEC 27001:2013; (5) Center for Internet Security (CIS) Controls, v. 7.1, Implementation Group 1 or higher; (6) AICPA System and Organization Controls (SOC) 2, Type 2; and (7) Payment Card Industry Data Security Standard (PCI DSS), v3.2.1. The Provider will provide to the LEA on an annual basis and upon written request demonstration of successful certification of these alternative standards in the form of a national or international Certification document; an Authorization to Operate (ATO) issued by a state or federal agency, or by a recognized security standards body; or a Preliminary Authorization to Operate (PATO) issued by the FedRAMP Joint Authorization Board (JAB).

\*ProQuest does not require the use of Student Data or PII for use of the ProQuest products and a facilitated walk-through of ProQuest's systems shall satisfy the obligations with respect to the provision of a national or international audit certification.

- 8. In the case of a data breach, as a part of the security breach notification outlined in Article V, Section 4(1), the Provider agrees to provide the following additional information:
  - i. The estimated number of students and teachers affected by the breach, if any.
- 9. The parties agree to add the following categories into the definition of Student Data: the name of the student's parents or other family members, place of birth, social media address, unique pupil identifier, and credit card account number, insurance account number, and financial services account number.
- 10. In Article V, Section 1 Data Storage: New Hampshire does not require data to be stored within the United States.

**EXHIBIT "I" – TEACHER DATA**

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	
Communications	Online communications that are captured (emails, blog entries)	
Demographics	Date of Birth	
	Place of Birth	
	Social Security Number	
	Ethnicity or race	
	Other demographic information-Please specify:	
Personal Contact Information	Personal Address	
	Personal Email	
	Personal Phone	
Performance evaluations	Performance Evaluation Information	
Schedule	Teacher scheduled courses	
	Teacher calendar	
Special Information	Medical alerts	
	Teacher disability information	
	Other indicator information-Please specify:	
Teacher Identifiers	Local (School district) ID number	
	State ID number	
	Vendor/App assigned student ID number	
	Teacher app username	
	Teacher app passwords	
Teacher In App Performance	Program/application performance	
Teacher Survey Responses	Teacher responses to surveys or questionnaires	
Teacher work	Teacher generated content; writing, pictures etc.	
	Other teacher work data -Please specify:	
Education	Course grades from schooling	
	Other transcript data -Please specify:	
Other	Please list each additional data element used, stored or collected by your application	

**EXHIBIT “A1”**  
**DESCRIPTION OF SERVICES**

Platform:      **ProQuest Academic Platform**

Intended for use by K-12 Educators and upper level students age 13 and above.

Anonymous browsing of materials is facilitated on the on-line platform. Authenticated Teachers and Students (age 13 and older) may consent to the use of their email address during optional user account (**MyResearch**) set up enabling personalize features such as saved searches and alerts.

The responsively designed user interface offers access on any device at any time via your devices web-browser.

Some **User Survey Responses** may be captured through ProQuest Platform (Qualtrics Integration). Short user surveys are occasionally presented to users that request feedback on the features, functionality, or content in the service being used. No personal data is required and the user may choose not to respond.

Except as noted above, **no Student Data** is provided to ProQuest by its Customers nor required for purposes of performing or providing the services.

**No Pupil Records** are stored or accessed through the ProQuest® online research platform.

**Research Databases on the ProQuest® Platform**

**ABI Inform Global:** Quickly connects business researchers with more of the scholarly information that they need. ABI/INFORM Global contains the full text of thousands of journals, including essential scholarly journals, magazines and trade journals. Researchers increasingly need more than just scholarly journals to stay current and conduct their research thoroughly and effectively. This is why we have made it easy for them to also access thousands of dissertations, working papers, news sources, and much more.

**American Periodicals** is a foundational, richly cross-disciplinary resource for research into myriad aspects of American history, bringing unprecedented scope and scale to this type of content. It comprises 10M digitized page images from 1,800 historical serials spanning almost 250 years of American history, from the colonial period to the late-20th century. The broad cross-section of periodical types from the period includes popular titles, early professional journals, celebrations of Americana, and incisive social and political magazines. American Periodicals consists of two separately purchasable collections: American Periodicals Series Online and American Periodicals from the Center for Research Libraries

**Colonial State Papers:** Through collaboration with The National Archives of the United Kingdom, The Colonial State Papers offers access to over 7,000 hand-written documents and more than 40,000 bibliographic records with this incredible resource on Colonial History. In addition to Britain's colonial relations with the Americas and other European rivals for power, The Colonial State Papers also include coverage of the Caribbean and Atlantic world. This is an invaluable resource for scholars of Early American history, British colonial history, history of the Caribbean, maritime history, Atlantic trade, plantations and slavery.

**The Health & Medical Collection** is uniquely suited for libraries with users who require content for learning and researching biomedical science and related subject areas. Our content helps health science librarians meet the research needs of many audiences, whether they're supporting a clinical research study or providing faculty with instructional multimedia content to help students connect theory to practice.

**Literature Online (LION):** Literature Online offers an authoritative database of primary and critical texts matched with a specialist interface designed for literary research. Centuries of accurately reproduced primary texts and a wealth of relevant and important criticism and reference resources, such as scholarly journals and specially commissioned biographies helps serve the studying, teaching and researching of literature.

**ProQuest Central Student:** Designed to bring instant results to users across thousands of journals, magazines, newspapers, videos, and reports, ProQuest Central Student is a truly multidisciplinary resource. It can support every class in your program with coverage of 160 subjects including current events, literature and humanities, sciences, health, social sciences, and business. Designed to meet high school and college-prep programs.

**ProQuest Historical Newspapers:** Historical newspaper content from more than 50 premier stand-alone historical titles dating back to the 1700s and more than 55 million digitized pages. ProQuest historical Newspapers is the definitive newspaper archive that includes full-page and/or article images in easily downloadable PDFs. Titles include HNP Hartford Courant, HNP Atlanta Constitution, HNP Atlanta Constitution, HNP Atlanta Daily World, HNP Baltimore Afro-American, HNP Baltimore Sun, HNP Boston Globe, HNP Call Post, HNP Chicago Defender, HNP Chicago Tribune Original Years, HNP Chinese Newspaper Collections, HNP Christian Science Monitor, HNP Guardian and Observer, HNP Irish Times, HNP LA Sentinel, HNP LA Times, HNP New York Times, HNP New York Tribune 1842-1922, HNP Norfolk Journal and Guide, HNP NY Amsterdam News, HNP Philadelphia Tribune, HNP Pittsburgh Courier, HNP Scotsman, HNP SF Chronical, HNP Times of India, HNP Wall Street Journal, HNP Washington Post.

**STEM Database** delivers a wide-ranging collection of more than 500 magazines and journals designed to support studies in science, tech, engineering and math subject areas. Disciplines covered include earth, life, physical, medical, mathematics and applied sciences, such as engineering.

**Newspapers & U.S. Major Dailies:** Recent newspaper content is among the most sought-after primary source material in research. ProQuest offers exclusive and preferred access to the five most respected

U.S, national and regional newspapers: *The New York Times*, *Washington Post*, *Los Angeles Times*, *Chicago Tribune*, and *the Wall Street Journal*.

**The Vogue Archive** comprises the backfile of the US edition of Vogue magazine from 1892 to the present day, reproduced in high-resolution color page images.

**Women's Magazine Archive Collections:** *Women's Magazine Archive* consists of two collections, each spotlighting a set of titles whose names still resonate today: Collection 1: *Better Homes & Gardens*, *Good Housekeeping*, *Ladies' Home Journal*, *Parents*, *Redbook*, *Chatelaine* (Canada); Collection 2: *Cosmopolitan*, *Essence*, *Seventeen*, *Town & Country*, *Woman's Day*, *Women's International Network News*. In all, *Women's Magazine Archive* will deliver some 850,000 pages per collection. The content supports research across disciplines, providing unique perspectives on social history, law, health, politics, the arts, and more.

**EXHIBIT “B1”**  
**SCHEDULE OF DATA**

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	X
	Other application technology meta data-Please specify:	N/A
Application Use Statistics	Meta data on user interaction with application	X
Assessment	Standardized test scores	N/A
	Observation data	N/A
	Other assessment data-Please specify:	N/A
Attendance	Student school (daily) attendance data	N/A
	Student class attendance data	N/A
Communications	Online communications that are captured (emails, blog entries)	N/A
Conduct	Conduct or behavioral data	N/A
Demographics	Date of Birth	N/A
	Place of Birth	N/A
	Gender	N/A
	Ethnicity or race	N/A
	Language information (native, preferred or primary language spoken by student)	N/A
	Other demographic information-Please specify:	N/A
Enrollment	Student school enrollment	N/A
	Student grade level	N/A
	Homeroom	N/A
	Guidance counselor	N/A
	Specific curriculum programs	N/A
	Year of graduation	N/A
	Other enrollment information-Please specify:	N/A
Parent/Guardian Contact Information	Address	N/A
	Email	N/A
	Phone	N/A
Parent/Guardian ID	Parent ID number (created to link parents to students)	N/A

Category of Data	Elements	Check if used by your system
Parent/Guardian Name	First and/or Last	N/A
Schedule	Student scheduled courses	N/A
	Teacher names	N/A
Special Indicator	English language learner information	N/A
	Low income status	N/A
	Medical alerts	N/A
	Student disability information	N/A
	Specialized education services (IEP or 504)	N/A
	Living situations (homeless/foster care)	N/A
	Other indicator information-Please specify:	N/A
Category of Data	Elements	Check if used by your system
Student Contact Information	Address	N/A
	*Email	X
	Phone	N/A
Student Identifiers	Local (School district) ID number	N/A
	State ID number	N/A
	Vendor/App assigned student ID number	N/A
	Student app username	N/A
	*Student app passwords	X
Student Name	**First and/or Last	X
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	N/A
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	N/A
Student Survey Responses	**Student responses to surveys or questionnaires	X
Student work	Student generated content; writing, pictures etc.	N/A

Category of Data	Elements	Check if used by your system
	Other student work data - Please specify:	N/A
Transcript	Student course grades	N/A
	Student course data	N/A
	Student course grades/performance scores	N/A
	Other transcript data -Please specify:	N/A

Category of Data	Elements	Check if used by your system
Transportation	Student bus assignment	N/A
	Student pick up and/or drop off location	N/A
	Student bus card ID number	N/A
	Other transportation data - Please specify:	N/A
		N/A
Other	Please list each additional data element used, stored or collected by your application	X

Other:

- **Admin Portal:** This library administration portal captures name (optional), email address, and passwords of library administrators.
- **Institutional Log-In Authentication (Optional).** A single ProQuest generated user name and password is provided to LEAs who chose this method as their authentication option. No Student Data, Pupil Records or other PII is captured or used .
- **\*User Personalization (MyResearch).** Where an authorized user (student, faculty or staff) opts to populate a user account to have access to personalization features of the service (such as saved documents, saved searches, alerts, RSS feeds) a user email address and password will be captured and verified at the time of account set up.
- **\*\*User Survey Responses** (Qualtrics Integration) may be presented to users, and are entirely optional. No user data is required to participate in the survey. Users are asked to provide a First Name and email address if they agree to provide further feedback to ProQuest.

The Provider may update the categories of data collected in Exhibit B after execution of this Agreement by providing notice to the LEA (and Subscribing LEAs applicable) of the updated categories of Student Data collected through a revised Exhibit B, which will thereafter become a part of the DPA and supersede the prior Exhibit B.

ProQuest Platform  
v. 20Nov2020/jd



**EXHIBIT “A2”**  
**DESCRIPTION OF SERVICES**

**ProQuest® K-12 Guided Research Student Interface**  
**(ProQuest Platform)**

The Guided Research Interface is offered for those ProQuest® database and reference services that are intended for use by students and teachers in K-12 schools.

No Student Data (as defined on Exhibit C) is collected from Customer or individual students when the products are accessed through the student interface.

The **SIRS®** and **e Library®** reference products may be accessed through the Guided Research interface described in this Exhibit or via the ProQuest Platform academic interface. For information about the ProQuest academic interface, please see the separate Exhibits outlining the features and functionality native to the ProQuest Platform.

**Reference Products with Guided Research Interface Available**

**e Library** is an online research service that helps simplify the research process and empowers novice researchers to more easily and efficiently choose their research topic and find authoritative information to support their research claim. It delivers one of the largest collections of periodical and digital media content editorially selected to support novice researchers. It includes more than 11,000 editor-created Research Topics pages deliver the essential elements on a vast array of people, places, historical events and eras, literary genres, current events, broad curricular themes and much more. Students can access primary and scholarly sources, and all content is in 100% full text. 1,700+ magazines, newspapers, transcripts and digitized reference book content, more than seven million images, maps, websites, videos and interactive simulations, all expertly curated by ProQuest editors.

**SIRS Discoverer** is a multidisciplinary topical research database specifically designed for upper elementary and middle school learners, researchers, and educators covering curriculum areas such as, history, health, language arts, math, science, social studies, and technology. All newspaper, magazine, and reference book content is 100% full text, editorially-selected and indexed from over 2,200 reliable, high-quality global sources. The collection includes vetted educational Websites and reference materials such as the Compton's by Britannica encyclopedia and DK Eyewitness books. Trusted periodical titles include Ranger Rick, Highlights for Children, Monkeyshines, New Moon, PopSci for Kids and many others.

**SIRS Issues Researcher** - When it comes to helping novice researchers understand the major issues of the day, SIRS® Issues Researcher stands apart by offering balanced content selections from more than 2,000 international sources. Analysis and opinions cover the pros, cons, and everything in between of 360+ social, scientific, health, historic, economic, and political issues. Editorially curated and created content including engaging Essential Questions, and viewpoint articles help build a solid foundation for

understanding complex global issues. Documents and graphics in SIRS Issues Researcher are carefully selected according to strict SIRS criteria for content reliability, relevance, and age-appropriateness. Titles include American History, The Christian Science Monitor, Economist, Foreign Affairs, Financial Times, Global Viewpoint, Maclean's, National Geographic, and Newsweek.

Legacy products: SIRS Government Reporter, SIRS Renaissance and SKS Package can now be found in SIRS Issues Researcher.

v. 20Nov2020/jd

## EXHIBIT “B2”

### SCHEDULE OF DATA

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	X
	Other application technology meta data-Please specify:	N/A
Application Use Statistics	Meta data on user interaction with application	X
Assessment	Standardized test scores	N/A
	Observation data	N/A
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	N/A
	Student class attendance data	N/A
Communications	Online communications that are captured (emails, blog entries)	N/A
Conduct	Conduct or behavioral data	N/A
Demographics	Date of Birth	N/A
	Place of Birth	N/A
	Gender	N/A
	Ethnicity or race	N/A
	Language information (native, preferred or primary language spoken by student)	N/A
	Other demographic information-Please specify:	N/A
Enrollment	Student school enrollment	N/A
	Student grade level	N/A
	Homeroom	N/A
	Guidance counselor	N/A
	Specific curriculum programs	N/A
	Year of graduation	N/A
	Other enrollment information-Please specify:	N/A
Parent/Guardian Contact Information	Address	N/A
	Email	N/A
	Phone	N/A
Parent/Guardian ID	Parent ID number (created to link parents to students)	N/A

Category of Data	Elements	Check if used by your system
Parent/Guardian Name	First and/or Last	N/A
Schedule	Student scheduled courses	N/A
	Teacher names	N/A
Special Indicator	English language learner information	N/A
	Low income status	N/A
	Medical alerts	N/A
	Student disability information	N/A
	Specialized education services (IEP or 504)	N/A
	Living situations (homeless/foster care)	N/A
	Other indicator information-Please specify:	N/A
Category of Data	Elements	Check if used by your system
Student Contact Information	Address	N/A
	Email	N/A
	Phone	N/A
Student Identifiers	Local (School district) ID number	N/A
	State ID number	N/A
	Vendor/App assigned student ID number	N/A
	Student app username	N/A
	Student app passwords	N/A
Student Name	First and/or Last	N/A
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	N/A
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	N/A
Student Survey Responses	Student responses to surveys or questionnaires	N/A
Student work	Student generated content; writing, pictures etc.	N/A

Category of Data	Elements	Check if used by your system
	Other student work data - Please specify:	N/A
Transcript	Student course grades	N/A
	Student course data	N/A
	Student course grades/performance scores	N/A
	Other transcript data -Please specify:	N/A

Category of Data	Elements	Check if used by your system
Transportation	Student bus assignment	N/A
	Student pick up and/or drop off location	N/A
	Student bus card ID number	N/A
	Other transportation data - Please specify:	N/A
		N/A
Other	Please list each additional data element used, stored or collected by your application	X

Other: Information Gathered for the Guided Research interface

- **Admin Portal:** This library administration portal captures name (optional), email address, and passwords of library administrators.
- **Institutional Log-In Authentication (Optional).** A single ProQuest generated user name and password is provided to LEAs who chose this method as their authentication option. No Student Data, Pupil Records or other PII is captured or used .
- **User Personalization.** These features are not available when users access the reference or research service via the Guided Research Student Interface. Personalization features remain available when products are offered through the ProQuest Platform. See separate Exhibits for ProQuest Platform.

The Provider may update the categories of data collected in Exhibit B after execution of this Agreement by providing notice to the LEA (and Subscribing LEAs applicable) of the updated categories of Student Data collected through a revised Exhibit B, which will thereafter become a part of the DPA and supersede the prior Exhibit B.

Guided Research  
v. 20Nov2020

**EXHIBIT “A3”**  
**DESCRIPTION OF SERVICES**

Intended for use by students and teachers in K-12 schools. No Student Data (as defined on Exhibit C) is collected from Customer or individual students when the products are accessed through the student interface.

**CultureGrams Online** (“CultureGrams”) is a leading online reference database for concise and reliable cultural information on the countries of the world. With world events increasingly affecting our lives, it's more important than ever to educate students about the world around them.

CultureGrams provides country reports that go beyond mere facts and figures to deliver a one-of-a-kind perspective on daily life and culture, including the background, customs, and lifestyles of the world's people. Individual reports covering 200+ countries, all 50 United States, and the Canadian provinces, are written and reviewed by in-country experts and are updated as new information becomes available, so you can be sure you're offering only the very best, most current information to staff and students.

v. 20Nov2020/jd

## EXHIBIT “B3”

### SCHEDULE OF DATA

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	X
	Other application technology meta data-Please specify:	N/A
Application Use Statistics	Meta data on user interaction with application	X
Assessment	Standardized test scores	N/A
	Observation data	N/A
	Other assessment data-Please specify:	N/A
Attendance	Student school (daily) attendance data	N/A
	Student class attendance data	N/A
Communications	Online communications that are captured (emails, blog entries)	N/A
Conduct	Conduct or behavioral data	N/A
Demographics	Date of Birth	N/A
	Place of Birth	N/A
	Gender	N/A
	Ethnicity or race	N/A
	Language information (native, preferred or primary language spoken by student)	N/A
	Other demographic information-Please specify:	N/A
Enrollment	Student school enrollment	N/A
	Student grade level	N/A
	Homeroom	N/A
	Guidance counselor	N/A
	Specific curriculum programs	N/A
	Year of graduation	N/A
	Other enrollment information-Please specify:	N/A
Parent/Guardian Contact Information	Address	N/A
	Email	N/A
	Phone	N/A
Parent/Guardian ID	Parent ID number (created to link parents to students)	N/A

Category of Data	Elements	Check if used by your system
Parent/Guardian Name	First and/or Last	N/A
Schedule	Student scheduled courses	N/A
	Teacher names	N/A
Special Indicator	English language learner information	N/A
	Low income status	N/A
	Medical alerts	N/A
	Student disability information	N/A
	Specialized education services (IEP or 504)	N/A
	Living situations (homeless/foster care)	N/A
	Other indicator information-Please specify:	N/A
Category of Data	Elements	Check if used by your system
Student Contact Information	Address	N/A
	Email	N/A
	Phone	N/A
Student Identifiers	Local (School district) ID number	N/A
	State ID number	N/A
	Vendor/App assigned student ID number	N/A
	Student app username	N/A
	Student app passwords	N/A
Student Name	First and/or Last	N/A
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	N/A
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	N/A
Student Survey Responses	Student responses to surveys or questionnaires	N/A
Student work	Student generated content; writing, pictures etc.	N/A

Category of Data	Elements	Check if used by your system
	Other student work data - Please specify:	N/A
Transcript	Student course grades	N/A
	Student course data	N/A
	Student course grades/performance scores	N/A
	Other transcript data -Please specify:	N/A

Category of Data	Elements	Check if used by your system
Transportation	Student bus assignment	N/A
	Student pick up and/or drop off location	N/A
	Student bus card ID number	N/A
	Other transportation data - Please specify:	N/A
		N/A
Other	Please list each additional data element used, stored or collected by your application	X

Other:

- **Admin Portal:** This library administration portal captures name (optional), email address, and passwords of library administrators.
- **Institutional Log-In Authentication (Optional).** A single ProQuest generated user name and password is provided to LEAs who chose this method as their authentication option. No Student Data, Pupil Records or other PII is captured or used .
- **User Personalization.** No personalization features are available for CultureGrams.

The Provider may update the categories of data collected in Exhibit B after execution of this Agreement by providing notice to the LEA (and Subscribing LEAs applicable) of the updated categories of Student Data collected through a revised Exhibit B, which will thereafter become a part of the DPA and supersede the prior Exhibit B.

CultureGrams  
v. 20Nov2020/jd

**EXHIBIT “A4”**  
**DESCRIPTION OF SERVICES**

**Platform/Services: Alexander Street and Alexander Street Video**

Intended for use by Colleges, Universities, as well as K-12 Educators and upper level students age 13 and above.

Anonymous searching and browsing of content is facilitated on the on-line platform. No **Student Data** or **Pupil Data** is required to use the services in this mode.

Authenticated Teachers and Students (age 13 and older) may consent to the use of a display name, email address and their chosen password during optional user account set up enabling personalized features on this service. The personalization features include the ability to create and save playlists, video clips and bookmarks related to content within the applicable service.

There is an optional LTI app that uses LTI 1.0 to allow embedding of links to content in the Customer’s Learning Management System (LMS) so that students can access the content using their credentials on the learning management system. ProQuest does not use, collect or store any individual identifying data in this process as the authentication is handled through the LMS.

Except as noted above, **no Student Data** is provided to ProQuest by its Customers nor required for purposes of performing or providing the services.

**No Pupil Records** are stored or accessed through any of the Alexander Street™ services.

**Example Alexander Street Offerings**

*ProQuest’s **Alexander Street** products are curated, discipline-focused, primary-source collections, websites and streaming media for learning and research. The following are examples of available databases and is not an exhaustive list. The above data uses and functionality remain the same across the services unless otherwise noted.*

**Academic Video Online (AVON)** is the most comprehensive video subscription available to libraries. It delivers more than 68,000 titles spanning the widest range of subject areas including anthropology, business, counseling, film, health, history, music, and more. More than 14,000 titles are exclusive to Alexander Street.

**American History in Video** includes 2,000 total hours of streaming video content, including newsreels and documentaries from United Newsreel and Universal Newsreel, PBS, California Newsreel, Bullfrog Films, Documentary Educational Resources, Pennebaker Hegedus Films, The History Channel®, and others.



**\*Harper's Weekly Series** represents the full-text of America's leading 19th century illustrated newspaper: 1857-1912.

**Music Online Listening** is a comprehensive and highest quality streaming audio collection to support the teaching and research of music. It currently provides academic libraries with streaming access to over 10 million tracks of audio recordings, and is growing monthly as new recordings are added.

**Theatre Performance and Design Collection** is a comprehensive, international collection that covers all aspects of theater from production and design to performance. It brings together Alexander Street's premiere collections of video performances, audio dramas, and designs that combine to bring the brilliance of stage into the classrooms.

**Theatre and Drama Premium** bridges the gap between Literature and Theatre departments, serving students and faculty in many disciplines, such as theatre, literature, performance studies, theatrical design, dramatic writing, and more. The collection includes the entire contents of our leading drama text collections, audio collections and video collections.

\*Asterisked services do not provide any of the personalization features or functionality. No Student Data or Pupil Records are captured.

v. 20Nov2020/jd

**EXHIBIT “B4”****SCHEDULE OF DATA**

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	X
	Other application technology meta data-Please specify:	n/a
Application Use Statistics	Meta data on user interaction with application	X
Assessment	Standardized test scores	n/a
	Observation data	n/a
	Other assessment data-Please specify:	n/a
Attendance	Student school (daily) attendance data	n/a
	Student class attendance data	n/a
Communications	Online communications that are captured (emails, blog entries)	n/a
Conduct	Conduct or behavioral data	n/a
Demographics	Date of Birth	n/a
	Place of Birth	n/a
	Gender	n/a
	Ethnicity or race	n/a
	Language information (native, preferred or primary language spoken by student)	n/a
	Other demographic information-Please specify:	n/a
Enrollment	Student school enrollment	n/a
	Student grade level	n/a
	Homeroom	n/a
	Guidance counselor	n/a
	Specific curriculum programs	n/a
	Year of graduation	n/a
	Other enrollment information-Please specify:	n/a
Parent/Guardian Contact Information	Address	n/a
	Email	n/a
	Phone	n/a
Parent/Guardian ID	Parent ID number (created to link parents to students)	n/a

Category of Data	Elements	Check if used by your system
Parent/Guardian Name	First and/or Last	n/a
Schedule	Student scheduled courses	n/a
	Teacher names	n/a
Special Indicator	English language learner information	n/a
	Low income status	n/a
	Medical alerts	n/a
	Student disability information	n/a
	Specialized education services (IEP or 504)	n/a
	Living situations (homeless/foster care)	n/a
	Other indicator information-Please specify:	n/a
Category of Data	Elements	Check if used by your system
Student Contact Information	Address	n/a
	Email	x
	Phone	n/a
Student Identifiers	Local (School district) ID number	n/a
	State ID number	n/a
	Vendor/App assigned student ID number	n/a
	Student app username	X
	Student app passwords	X
Student Name	First and/or Last	n/a
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	n/a
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	n/a
Student Survey Responses	Student responses to surveys or questionnaires	n/a
Student work	Student generated content; writing, pictures etc.	n/a

Category of Data	Elements	Check if used by your system
	Other student work data - Please specify:	n/a
Transcript	Student course grades	n/a
	Student course data	n/a
	Student course grades/performance scores	n/a
	Other transcript data -Please specify:	n/a

Category of Data	Elements	Check if used by your system
Transportation	Student bus assignment	n/a
	Student pick up and/or drop off location	n/a
	Student bus card ID number	n/a
	Other transportation data - Please specify:	n/a
Other	Please list each additional data element used, stored or collected by your application	X

Other: Alexander Street offerings capture the following information:

- **Administration Portal:** This library administration portal captures name (optional), email address, and passwords of library administrators.
- **Institutional Log-In Authentication (Optional).** A single ProQuest generated user name and password is provided to LEAs who chose this method as their authentication option. No Student Data, Pupil Records or other PII is captured or used .
- **User Personalization.** Where an authorized user (student, faculty or staff) opts to populate a user account to have access to personalization features of the service (such as creation of playlists or video clips) a user email address, display name and password will be captured at the time of account set up.

The Provider may update the categories of data collected in Exhibit B after execution of this Agreement by providing notice to the LEA (and Subscribing LEAs applicable) of the updated categories of Student Data collected through a revised Exhibit B, which will thereafter become a part of the DPA and supersede the prior Exhibit B.

Alexander Street  
v. 20Nov2020/jd

**EXHIBIT “A5”**  
**DESCRIPTION OF SERVICES**

Platform: **History Vault Platform**

Intended for use by K-12 Educators and upper level students age 13 and above.

Anonymous browsing of materials is facilitated on the on-line platform. Authenticated Teachers and Students (age 13 and older) may consent to the use of their email address during optional user account (User Profile) set up enabling personalize features such as saved searches and documents.

The responsively designed user interface offers access on any device at any time via your devices web-browser.

Some **User Survey Responses** may be captured through ProQuest Platform (Qualtrics Integration). Short user surveys are occasionally presented to users that request feedback on the features, functionality, or content in the service being used. No personal data is required and the user may choose not to respond.

Except as noted above, **no Student Data** is provided to ProQuest by its Customers nor required for purposes of performing or providing the services.

**No Pupil Records** are stored or accessed through History Vault research platform.

**ProQuest History Vault Research Databases**

This award-winning, continuously-growing digitized collection of manuscript and archival materials now has over 20 million pages in 51 different modules. Created in partnership with renowned archival institutions, History Vault gives students and researchers a firsthand look at pivotal moments in history through the power of primary sources. Collections include:

History Vault: American Indians and American West, 1809-1971

History Vault: American Politics and Society from Kennedy to Watergate, 1960-1975

History Vault: FBI Confidential Files and Radical Politics in the U.S., 1945-1972

History Vault: Immigration: Records of the INS, 1880-1930

History Vault: Margaret Sanger Papers

History Vault: NAACP Papers: The NAACP's Major Campaigns - Education, Voting, Housing, Employment, Armed Forces

History Vault: NAACP Papers: The NAACP's Major Campaigns - Scottsboro, Anti-Lynching, Criminal Justice, Peonage, Labor and Segregation and Discrimination Complaints and Responses

History Vault: Progressive Era: Reform, Regulation, and Rights

History Vault: Struggle for Women's Rights, Organizational Records, 1880-1990

History Vault: Students for a Democratic Society, Vietnam Veterans Against the War, and the Anti-Vietnam War Movement

History Vault: Vietnam War and American Foreign Policy, 1960-1975

History Vault: Women at Work during World War II: Rosie the Riveter and the Women's Army Corps

This is a representative list based on subscriptions adopted in your state as of the revision date of this Schedule.  
Additional Collections are available and conform to the user interface and data capture parameters outlined in these  
Schedules A & B.

Rev. 20Nov2020/jd

## **EXHIBIT “B5”**

### SCHEDULE OF DATA

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	X
	Other application technology meta data-Please specify:	N/A
Application Use Statistics	Meta data on user interaction with application	X
Assessment	Standardized test scores	N/A
	Observation data	N/A
	Other assessment data-Please specify:	N/A
Attendance	Student school (daily) attendance data	N/A
	Student class attendance data	N/A
Communications	Online communications that are captured (emails, blog entries)	N/A
Conduct	Conduct or behavioral data	N/A
Demographics	Date of Birth	N/A
	Place of Birth	N/A
	Gender	N/A
	Ethnicity or race	N/A
	Language information (native, preferred or primary language spoken by student)	N/A
Enrollment	Other demographic information-Please specify:	N/A
	Student school enrollment	N/A
	Student grade level	N/A
	Homeroom	N/A
	Guidance counselor	N/A
	Specific curriculum programs	N/A
Parent/Guardian Contact Information	Year of graduation	N/A
	Other enrollment information-Please specify:	N/A
	Address	N/A
Parent/Guardian ID	Email	N/A
	Phone	N/A
Parent/Guardian ID	Parent ID number (created to link parents to students)	N/A

Category of Data	Elements	Check if used by your system
Parent/Guardian Name	First and/or Last	N/A
Schedule	Student scheduled courses	N/A
	Teacher names	N/A
Special Indicator	English language learner information	N/A
	Low income status	N/A
	Medical alerts	N/A
	Student disability information	N/A
	Specialized education services (IEP or 504)	N/A
	Living situations (homeless/foster care)	N/A
	Other indicator information-Please specify:	N/A
Category of Data	Elements	Check if used by your system
Student Contact Information	Address	N/A
	*Email	X
	Phone	N/A
Student Identifiers	Local (School district) ID number	N/A
	State ID number	N/A
	Vendor/App assigned student ID number	N/A
	Student app username	N/A
	Student app passwords	N/A
Student Name	**First and/or Last	X
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	N/A
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	N/A
Student Survey Responses	Student responses to surveys or questionnaires	X
Student work	Student generated content; writing, pictures etc.	N/A

Category of Data	Elements	Check if used by your system
	Other student work data - Please specify:	N/A
Transcript	Student course grades	N/A
	Student course data	N/A
	Student course grades/performance scores	N/A
	Other transcript data -Please specify:	N/A

Category of Data	Elements	Check if used by your system
Transportation	Student bus assignment	N/A
	Student pick up and/or drop off location	N/A
	Student bus card ID number	N/A
	Other transportation data - Please specify:	N/A
Other	Please list each additional data element used, stored or collected by your application	X

Other:

- **Admin Portal:** This library administration portal captures name (optional), email address, and passwords of library administrators.
- **Institutional Log-In Authentication (Optional).** A single ProQuest generated user name and password is provided to LEAs who chose this method as their authentication option. No Student Data, Pupil Records or other PII is captured or used.
- **\*User Personalization (User Profile).** Where an authorized user (student, faculty or staff) opts to populate a user account to have access to personalization features of the service (such as saved documents, saved searches, and recent searches) a user email address and password will be captured at the time of account set up.
- **\*\*User Survey Responses** may be captured through the platform (Qualtrics Integration). Short user surveys are occasionally presented to users that request feedback on the features, functionality, or content in the service being used. No personal data is required and the user may choose not to respond.

The Provider may update the categories of data collected in Exhibit B after execution of this Agreement by providing notice to the LEA (and Subscribing LEAs applicable) of the updated categories of Student Data collected through a revised Exhibit B, which will thereafter become a part of the DPA and supersede the prior Exhibit B.

## **EXHIBIT “A6”**

### **DESCRIPTION OF SERVICES**

#### **Platform: ProQuest Ebook Central**

Intended for use by K-12 Educators and upper level students age 13 and above.

Anonymous browsing of Ebooks is facilitated on the on-line platform. Authenticated Teachers and Students (age 13 and older) may consent to the use of their email address during optional user account set up enabling personalized features on this service and there is an optional eBook reader app that uses the Student Data as indicated on Schedule B.

Except as noted in the previous paragraph, **no Student Data** is provided to ProQuest by its Customers nor required for purposes of performing or providing the services.

**No Pupil Records** are stored or accessed through any of the Ebook Central systems.

#### **Example Offerings on the ProQuest® Ebook Central Platform**

*These are examples, additional Ebook Databases as well as purchased titles and collections are available on this platform, all described functionality remains the same.*

**Academic Complete Subscription Database:** Academic Complete is ProQuest’s foundational, multidisciplinary aggregated Ebook subscription database provides users 24/7, unlimited access to academic Ebooks. With more than 180,000 titles curated by our in-house librarians, it offers libraries an affordable, critical mass of content to serve the needs of academic researchers worldwide.

**Schools and Educators Complete Subscription Database:** This Ebook database offers a foundational base of more than 14,700 ebooks for K-12 students and teachers that are available anytime and anywhere. Key topics for students include history, art, science, music, math, computers, literature, writing, religion, and fiction. Teachers benefit from such subjects as common core, distance learning, classroom management, curriculum planning, educational technology, tests and measurements; child development, psychology and disabilities, and more.

**Optional Library Thing Book Cover Widget:** A Book Display Widget that is interoperable with the ProQuest® Ebook Central platform and highlights your collections and puts them front and center on your library’s homepage. Patrons just click on the image of the book cover to go directly to that title in your catalog.

No Faculty or Student Data or Records are accessed, used or stored in connection with the Widget



## EXHIBIT “B6”

### SCHEDULE OF DATA

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	X
	Other application technology meta data-Please specify:	N/A
Application Use Statistics	Meta data on user interaction with application	X
Assessment	Standardized test scores	N/A
	Observation data	N/A
	Other assessment data-Please specify:	N/A
Attendance	Student school (daily) attendance data	N/A
	Student class attendance data	N/A
Communications	Online communications that are captured (emails, blog entries)	N/A
Conduct	Conduct or behavioral data	N/A
Demographics	Date of Birth	N/A
	Place of Birth	N/A
	Gender	N/A
	Ethnicity or race	N/A
	Language information (native, preferred or primary language spoken by student)	X
	Other demographic information-Please specify:	N/A
Enrollment	Student school enrollment	N/A
	Student grade level	N/A
	Homeroom	N/A
	Guidance counselor	N/A
	Specific curriculum programs	N/A
	Year of graduation	N/A
	Other enrollment information-Please specify:	N/A
Parent/Guardian Contact Information	Address	N/A
	Email	N/A
	Phone	N/A
Parent/Guardian ID	Parent ID number (created to link parents to students)	N/A

Category of Data	Elements	Check if used by your system
Parent/Guardian Name	First and/or Last	N/A
Schedule	Student scheduled courses	N/A
	Teacher names	N/A
Special Indicator	English language learner information	N/A
	Low income status	N/A
	Medical alerts	N/A
	Student disability information	N/A
	Specialized education services (IEP or 504)	N/A
	Living situations (homeless/foster care)	N/A
	Other indicator information-Please specify:	N/A
Category of Data	Elements	Check if used by your system
Student Contact Information	Address	N/A
	Email	X
	Phone	N/A
Student Identifiers	Local (School district) ID number	N/A
	State ID number	N/A
	Vendor/App assigned student ID number	N/A
	Student app username	X
	Student app passwords	X
Student Name	First and/or Last	X
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	N/A
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	N/A
Student Survey Responses	Student responses to surveys or questionnaires	N/A
Student work	Student generated content; writing, pictures etc.	N/A

Category of Data	Elements	Check if used by your system
	Other student work data - Please specify:	N/A
Transcript	Student course grades	N/A
	Student course data	N/A
	Student course grades/performance scores	N/A
	Other transcript data -Please specify:	N/A

Category of Data	Elements	Check if used by your system
Transportation	Student bus assignment	N/A
	Student pick up and/or drop off location	N/A
	Student bus card ID number	N/A
	Other transportation data - Please specify:	N/A
Other	Please list each additional data element used, stored or collected by your application	X

Other: Ebook Central captures:

- **LibCentral:** This library administration portal captures name, title, email address, and passwords of library administrators.
- **Patron Log-In Option.** Where Patron Log-In is chosen by the library as its user authentication method, ProQuest will receive library designated username and passwords for its users for the purposes of user authentication.
- **Single Sign-On or Patron Personalization.** Where an authorized user (student, faculty or staff) opts to populate a user account to have access to personalization features of the service (such as alerts or book checkouts) or uses the ereader app, a user email and password will be captured at the time of account set up.

The Provider may update the categories of data collected in Exhibit B after execution of this Agreement by providing notice to the LEA (and Subscribing LEAs applicable) of the updated categories of Student Data collected through a revised Exhibit B, which will thereafter become a part of the DPA and supersede the prior Exhibit B.

**EXHIBIT “A7”**  
**DESCRIPTION OF SERVICES**

Platform/Service: **ProQuest Research Companion (PQRC)**

No personal information is required to watch the videos or use the tools; once authenticated into the system, students may start viewing the learning modules and using the research tools.

A student account is required for: 1) tracking progress through the learning modules and 2) completing the assessment questions where the school administrator has activated the assessment tools.

At the time of account creation, ProQuest obtains the student email addresses and other information disclosed on Exhibit B for account setup described above. The email is stored for the purpose of sending a reminder about a forgotten password.

PQRC runs from the Student’s web browser and the responsive design means it’s adaptable to all devices—laptops, tablets, and smart phones.

Except as noted above, **no Student Data** is provided to ProQuest by its Customers nor required for purposes of performing or providing the services.

Except for the limited assessment information captured by the application, **No Pupil Records** are captured, stored or accessed through PQRC.

**ProQuest Research Companion**

An award-winning, cloud-based information literacy solution that enables educators and librarians to guide students through research projects efficiently, at every step. ProQuest Research Companion is designed to be easy, intuitive, and informative. It helps students develop their critical thinking skills to more effectively find, evaluate, and use information. Multimedia-based Learning Modules engage students to think more critically and creatively about their research, while the powerful, interactive Tools help students navigate through the research process.

**Learning Modules** - The material in the Learning Modules unit is presented in visually compelling, creative videos, and written in a conversational style that improves learning outcomes and maximizes retention. An assessment component is also available to measure student progress.

**Research Tools** - Research Companion’s simple Tools feature automates the basic parts of the research process by leveraging the power of ProQuest data sources, including Ulrich’s and Books In Print. Tools include a source evaluation aid, search aid, and revision aid to help students search, evaluate sources, and write more clearly and persuasively.

**Customization** - Customization features provide greater flexibility for educators to incorporate learning modules into their classrooms, workflow, and learning management systems.

v. 20Nov2020/jd

## **EXHIBIT “B7”**

### SCHEDULE OF DATA

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	X
	Other application technology meta data-Please specify:	N/A
Application Use Statistics	Meta data on user interaction with application	X
Assessment	Standardized test scores	N/A
	Observation data	N/A
	Other assessment data-Please specify: See below	X
Attendance	Student school (daily) attendance data	N/A
	Student class attendance data	N/A
Communications	Online communications that are captured (emails, blog entries)	N/A
Conduct	Conduct or behavioral data	N/A
Demographics	Date of Birth	N/A
	Place of Birth	N/A
	Gender	N/A
	Ethnicity or race	N/A
	Language information (native, preferred or primary language spoken by student)	N/A
	Other demographic information-Please specify:	N/A
Enrollment	Student school enrollment	N/A
	Student grade level	N/A
	Homeroom	N/A
	Guidance counselor	N/A
	Specific curriculum programs	N/A
	Year of graduation	N/A
	Other enrollment information-Please specify:	N/A
Parent/Guardian Contact Information	Address	N/A
	Email	N/A
	Phone	N/A
Parent/Guardian ID	Parent ID number (created to link parents to students)	N/A

Category of Data	Elements	Check if used by your system
Parent/Guardian Name	First and/or Last	N/A
Schedule	Student scheduled courses	N/A
	Teacher names	N/A
Special Indicator	English language learner information	N/A
	Low income status	N/A
	Medical alerts	N/A
	Student disability information	N/A
	Specialized education services (IEP or 504)	N/A
	Living situations (homeless/foster care)	N/A
	Other indicator information-Please specify:	N/A
Category of Data	Elements	Check if used by your system
Student Contact Information	Address	N/A
	Email	X
	Phone	N/A
Student Identifiers	Local (School district) ID number	N/A
	State ID number	N/A
	Vendor/App assigned student ID number	N/A
	Student app username	X
	Student app passwords	X
Student Name	First and/or Last	X
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	X
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	N/A
Student Survey Responses	Student responses to surveys or questionnaires	N/A
Student work	Student generated content; writing, pictures etc.	N/A

Category of Data	Elements	Check if used by your system
	Other student work data - Please specify:	N/A
Transcript	Student course grades	N/A
	Student course data	N/A
	Student course grades/performance scores	N/A
	Other transcript data -Please specify:	N/A

Category of Data	Elements	Check if used by your system
Transportation	Student bus assignment	N/A
	Student pick up and/or drop off location	N/A
	Student bus card ID number	N/A
	Other transportation data - Please specify:	N/A
		N/A
Other	Please list each additional data element used, stored or collected by your application	X

- **Admin Portal:** This library administration portal captures name (optional), email address, and passwords of library administrators.
- **Student Accounts:** If assessments features are activated by the library/school administrator for the account, Students may set up accounts that capture: First Name, Last Name, self-selected User Name, password and email address.
- **Assessment/ Student In App Performance:** If assessment capabilities are activated by the library/school administrator for the account, the application will evaluate whether the student watches instructional videos, measure student review of video research modules, and assign badges based on completion.

The Provider may update the categories of data collected in Exhibit B after execution of this Agreement by providing notice to the LEA (and Subscribing LEAs applicable) of the updated categories of Student Data collected through a revised Exhibit B, which will thereafter become a part of the DPA and supersede the prior Exhibit B.












# ProQuest MSAD51 final

Final Audit Report

2023-09-14

Created:	2023-08-21
By:	Ramah Hawley (rhawley@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAAi9quMTCdPkOejT_g8wyx7SJuzW5FoxMJ

## "ProQuest MSAD51 final" History

-  Document created by Ramah Hawley (rhawley@tec-coop.org)  
2023-08-21 - 1:25:20 PM GMT- IP address: 108.35.203.7
-  Document emailed to Shelly Dickey (shelly.dickey@clarivate.com) for signature  
2023-08-21 - 1:27:08 PM GMT
-  Email viewed by Shelly Dickey (shelly.dickey@clarivate.com)  
2023-08-21 - 1:30:47 PM GMT- IP address: 104.47.58.126
-  Document signing delegated to Dawn Branham (dawn.branham@clarivate.com) by Shelly Dickey (shelly.dickey@clarivate.com)  
2023-08-21 - 1:33:02 PM GMT- IP address: 99.8.89.200
-  Document emailed to Dawn Branham (dawn.branham@clarivate.com) for signature  
2023-08-21 - 1:33:02 PM GMT
-  Email viewed by Dawn Branham (dawn.branham@clarivate.com)  
2023-08-21 - 2:43:37 PM GMT- IP address: 104.47.55.126
-  Document e-signed by Dawn Branham (dawn.branham@clarivate.com)  
Signature Date: 2023-08-21 - 2:44:29 PM GMT - Time Source: server- IP address: 165.225.57.197
-  Document emailed to Dirk Van Curan (dvancuran@msad51.org) for signature  
2023-08-21 - 2:44:30 PM GMT
-  Email viewed by Dirk Van Curan (dvancuran@msad51.org)  
2023-09-14 - 7:07:52 PM GMT- IP address: 169.244.136.204
-  New document URL requested by Dirk Van Curan (dvancuran@msad51.org)  
2023-09-14 - 7:07:57 PM GMT- IP address: 169.244.136.204
-  Document e-signed by Dirk Van Curan (dvancuran@msad51.org)  
Signature Date: 2023-09-14 - 7:09:00 PM GMT - Time Source: server- IP address: 169.244.136.204



**Adobe Acrobat Sign**

✔ Agreement completed.

2023-09-14 - 7:09:00 PM GMT



**Adobe Acrobat Sign**

## Exhibit "G"

### New York

### ~~New York~~

1. 1. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
2. Student Data will be used by Provider exclusively to provide the Services identified in Exhibit A to the DPA.
3. Provider agrees to maintain the confidentiality and security of Student Data in accordance with LEA's Data Security and Privacy Policy. The LEA's Data Security Policy is attached hereto as Exhibit J. Each Subscribing LEA will provide its Data Security Policy to the Provider upon execution of Exhibit "E". Provider shall use industry standard security measures including encryption protocols that comply with New York law and regulations to preserve and protect Student Data and APPR Data. Provider must Encrypt Student Data and APPR Data at rest and in transit in accordance with applicable New York laws and regulations.
4. Provider represents that their Data Privacy and Security Plan can be found at the URL link listed in Exhibit K and is incorporated into this DPA. Provider warrants that its Data Security and Privacy Plan, at a minimum: (a) implements all applicable state, federal and local data privacy and security requirements; (b) has operational technical safeguards and controls in place to protect PII that it will receive under the service agreement; (c) complies with the LEA's parents bill of rights for data privacy and security; (d) requires training of all providers' employees, assignees and subprocessors who have Access to student data or APPR data; (e) ensures subprocessors are required to protect PII received under this service agreement; (f) specifies how data security and privacy incidents that implicate PII will be managed and ensuring prompt notification to the LEA, and (g) addresses Student Data return, [deletion and destruction.](#)  
[deletion and destruction.](#)
5. In addition to the requirements described in Paragraph 3 above, the Provider's Data Security and Privacy Plan shall be deemed to incorporate the LEA's Parents Bill of Rights for Data Security and Privacy, as found at the URL link identified in Exhibit J. The Subscribing LEA will provide its Parents Bill of Rights for Data Security and Privacy to the Provider upon execution of Exhibit "E".
6. All references in the DPA to "Student Data" shall be amended to include and state, "Student Data and [APPR Data.](#)"  
[APPR Data."](#)
7. To amend Article II, Section 5 to add: Provider shall ensure that its subprocessors agree that they do  
[\\_\\_\\_\\_\\_](#)



11. To amend Article IV, Section 7 to add: 'Notwithstanding the foregoing, Provider is prohibited from using Student Data or APPR data for any Commercial or Marketing Purpose as defined herein. And add after (iii) account holder, "which term shall not include students."
12. To replace Article V, Section 1 (Data Storage) to state: Student Data and APPR Data shall be stored within the United States and Canada only. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.
13. To replace Article V, Section 2 (Audits) to state: No more than once a year or following an unauthorized Access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA or its designee(s) to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA. The Provider will cooperate reasonably with the LEA or its designee(s) and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable Access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA.

Upon request by the New York State Education Department's Chief Privacy Officer (NYSED CPO), Provider shall provide the NYSED CPO with copies of its policies and related procedures that pertain to the protection of information. In addition, the NYSED CPO may require Provider to undergo an audit of its privacy and security safeguards, measures, and controls as they pertain to alignment with the requirements of New York State laws and regulations, and alignment with the NIST Cybersecurity Framework. Any audit required by the NYSED CPO must be performed by an independent third party at Provider's expense and the audit report must be provided to the NYSED CPO. In lieu of being subject to a required audit, Provider may provide the NYSED CPO with an industry standard independent audit report of Provider's privacy and security practices that was issued no more than twelve months before the date that the NYSED CPO informed Provider that it required Provider to undergo an audit. Failure to reasonably cooperate with any of the requirements in this provision shall be deemed a material breach of the DPA.

To amend the third sentence of Article V. Section 3 (Data Security) to read: The Provider shall implement security practices that are in alignment with the NIST Cybersecurity Framework v1.1 or any update to this Framework that is adopted by the New York State Department of Education.

14. To replace Article V. Section 4 (Data Breach) to state: In the event of a Breach as defined in 8 NYCRR Part 121.1 Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident or no more than 7 calendar days, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:
  - (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available: