FINALSITE STUDENT DATA PRIVACY AGREEMENT[1]

This Student Data Privacy Agreement ("**DPA**") is entered into on the date of full execution of the Order and Statement of Work ("**Effective Date**") and is entered into by and between the educational agency set forth below as identified in the signature block of this DPA ("**LEA**" or "**Customer**") and ACTIVE INTERNET TECHNOLOGIES, LLC, a Connecticut Corporation, d/b/a Finalsite, with offices at 655 Winding Brook Drive, Glastonbury, Connecticut, 06033 ("**Finalsite**") (jointly "**the Parties**", and each a "**Party**").

WHEREAS, Finalsite is providing digital services to LEA, as specified in certain contractual documents, including the applicable Master Terms and Conditions ("**Master Terms**"), each fully executed Order and Statement of Work, or under any services agreement or similar agreement (collectively, "**Agreement**"). Capitalized terms now otherwise defined in this DPA shall have the meanings ascribed to them in the Master Terms.

WHEREAS, Finalsite 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), Protection of Pupil Rights Amendment ("**PPRA**") 20 U.S.C. 1232h, applicable state privacy laws and regulations;

WHEREAS, Finalsite and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable data protection laws and regulations; and

WHEREAS, this DPA supplements the Agreement and in the event of any conflict between the terms of this DPA and the terms of the Agreement, the terms of this DPA prevail with regard to the specific subject matter of this DPA.

NOW THEREFORE, for good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties agree as follows:

1. Standard Clauses. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Finalsite, and other information specific to this DPA are contained in the Standard Clauses hereto.
2. Special Provisions. Supplemental State Terms and attached hereto as Exhibit F are hereby incorporated by reference into this DPA in their entirety.
3. Conflicts. In the event of a conflict between this DPA's Standard Clauses and applicable Supplemental State Terms, the Supplemental State Terms will control. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Agreement and Finalsite Terms of Service or Privacy Policy, the terms of this DPA shall control. This DPA amends, supersedes and replaces any prior agreement relating to data processing and/or data protection the Parties entered into.
4. Term. This DPA shall stay in effect for the term of the Agreement.
5. Services. The services to be provided by Finalsite to LEA pursuant to this DPA are detailed in Exhibit A.

[1] Modeled after the Student Data Privacy Consortium's set of National Data Processing Addendum for student data (Version 1.0).

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 LEA for this DPA is:

[*Please see the signature page of the Order and Statement of Work.*]

The designated representative for Finalsite for this DPA is:

[*Please see the signature page of the Order and Statement of Work.*]

IN WITNESS WHEREOF, LEA and Finalsite hereto agree, as evidenced by the signature page of the Order and Statement of Work to which this DPA is incorporated by reference, the Parties have executed this DPA as of the Effective Date.

1 STANDARD CLAUSES

ARTICLE 1 SCOPE AND PURPOSE

1.1 **Purpose of DPA**. The purpose of this DPA is to describe the Parties' duties and responsibilities related to Student Data, including compliance with Applicable Data Protection Laws. In performing the Services, for the purposes of FERPA, Finalsite shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by LEA. Finalsite shall be under the direct control and supervision of LEA with respect to its Processing of Student Data.

1.2 **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.

1.3 **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 2 DATA OWNERSHIP AND AUTHORIZED ACCESS

2.1 **Student Data Property of LEA**. As between LEA and Finalsite, all Student Data transmitted to Finalsite pursuant to the Agreement is and will continue to be the property of and under the control of LEA. Finalsite further acknowledges and agrees that all copies of such Student Data transmitted to Finalsite, 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 Agreement, shall remain the exclusive property of LEA.

2.2 **Parent Access**. 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 transfer student-generated content to a personal account, consistent with the functionality of services. Finalsite 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 LEA's request for Student Data in a student's records held by Finalsite to view or correct as necessary. In the event that a parent of a student or other individual contacts Finalsite to review any of the Student Data accessed pursuant to the Services, Finalsite shall refer the parent or individual to LEA, who will follow the necessary and proper procedures regarding the requested information, provided however, that Finalsite may also allow for direct access requests (but not correction or deletion rights) of Student Data and/or Education Records from a verified parent or guardian through tools available through Finalsite Services that permits users to access and/or manage their records.

2.3 **Separate Account**. To the extent applicable, if Student Generated Content is Processed by Finalsite as part of the Services, Finalsite may, at the request of LEA, transfer, or provide a mechanism for LEA to transfer, said Student Generated Content to a separate account created by the student.

2.4 **Third Party Requests.** Should a third party, including law enforcement or other government entities ("Requesting Party(ies)") contact Finalsite with a request for Student Data held by Finalsite pursuant to the Services, Finalsite shall redirect the Requesting Party to request Student Data directly from LEA and shall not provide the requested Student Data to the Requesting Party, unless

to the extent that Finalsite reasonably believes it is compelled to grant such access to the third party because the data disclosure is necessary: (i) pursuant to a court order or legal process, (ii) to comply with Applicable Data Protection Laws, (iii) to enforce the Agreement, or (iv) to protect the rights, property or personal safety of Finalsite's users, employees or others, or the security of the Services. Finalsite shall notify LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform LEA of the request.

2.5 **Subprocessors.** Finalsite shall enter into written agreements with all Subprocessors performing functions for Finalsite in order for Finalsite to provide the Services pursuant to the Agreement. LEA acknowledges and agrees that (a) Finalsite's Affiliates may be retained as Subprocessors, (b) Finalsite may engage its current Subprocessors listed in the customer portal on its website, as published by Finalsite and may be updated from time to time at https://www.finalsite.com/subprocessors; and (c) Finalsite and Finalsite's Affiliates respectively may engage third-party Subprocessors in connection with the provision of the Services.

ARTICLE 3 DUTIES OF LEA

3.1 **Provide Data in Compliance with Applicable Laws**. LEA warrants that it shall, in its use of and for the purposes of obtaining the Services, Process Student Data and provide Student Data in compliance with Applicable Data Protection Laws, as may be amended from time to time.

3.2 **Annual Notification of Rights**. If 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. Additionally, LEA represents, warrants, and covenants to Finalsite, as applicable, that LEA has (a) complied with the School Official Exemption, including, without limitation, informing parents in their Annual Notification of Rights that LEA defines "school official" to including service providers such as Finalsite and defines "legitimate educational interest" to include services such as the Services provided by Finalsite; (b) complied with the Directory Information Exemption, including, without limitation, informing parents and eligible students what information LEA deems to be Directory Information and may be disclosed and allowing parents and eligible students a reasonable amount of time to request that schools not disclose Directory Information about them; and (c) obtained all necessary parental, legal guardians', or eligible student written consent to share the Student Data with Finalsite, in each case, solely to enable Finalsite's operation of the Services.

3.3 **Reasonable Precautions**. LEA shall use reasonable administrative, physical and technical safeguards designed to secure usernames, passwords, and any other means of gaining access to the Services and hosted Student Data from unauthorized access, disclosure or acquisition by an unauthorized person.

3.4 **Unauthorized Access Notification**. LEA shall notify Finalsite promptly, within 72 hours, of any known or suspected unauthorized use or access of the Services. LEA will assist Finalsite in any efforts by Finalsite to investigate and respond to any unauthorized use or access.

ARTICLE 4 DUTIES OF FINALSITE

4.1 **Privacy Compliance**. Finalsite 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.

4.2 **Authorized Use**. The Student Data shared pursuant to the Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in Exhibit A or stated in the Agreement and/or otherwise authorized under the statutes referred to herein this DPA.

4.3 **Finalsite Employee Obligation**. Finalsite shall require all of Finalsite'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 Agreement. Finalsite agrees to require each employee or agent with access to Student Data to adhere to their confidentiality obligations with regard to Student Data.

4.4 **No Disclosure**. Finalsite 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 LEA or this DPA. This prohibition against disclosure shall not apply to (a) aggregate summaries of De-Identified Data, (b) Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, (c) to Subprocessors performing services on behalf of Finalsite pursuant to this DPA, (d) to authorized users of the Services, including parents or legal guardians, or (f) to protect the rights, property or personal safety of Finalsite's users, employees or others, or the security of the Services.

4.5 **De-Identified Data**. Finalsite agrees not to attempt to re-identify De-Identified Data. De-Identified Data may be used by Finalsite for those purposes allowed under FERPA and the following purposes: (a) assisting LEA or other governmental agencies in conducting research and other studies; and (b) research and development of Finalsite's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (c) for adaptive learning purposes and for customized student learning. Finalsite'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, Finalsite agrees not to transfer De-Identified Data to any party unless (i) that party agrees in writing not to attempt re-identification, and (ii) prior written notice has been given to LEA who has provided prior written consent for such transfer. Prior to publishing any document that names LEA explicitly or indirectly, Finalsite shall obtain LEA's written approval of the manner in which De-Identified Data is presented.

4.6 **Disposition of Data**. Upon written request from LEA, Finalsite shall dispose of or provide a mechanism for LEA to transfer Student Data obtained under the 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 LEA is received, Finalsite shall dispose of all Student Data after providing 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 3.3. LEA may employ a "**Directive for Disposition of Data**" form, a copy of which is attached hereto as Exhibit D. If LEA and Finalsite 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.

4.7 **Advertising Limitations**. Finalsite 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 Finalsite 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 5 DATA PROVISIONS

5.1 **Data Storage**. Where required by applicable law, Student Data shall be stored within the United States. Upon request of LEA, Finalsite will provide a list of the locations where Student Data is stored.

5.2 **Audits**. No more than once a year, or following a Security Incident, upon receipt of a written request from LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, at the cost of LEA, Finalsite will allow LEA's third party auditor to audit, during normal business hours and at a time convenient for Finalsite, 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 LEA ("**Security Audit**"). Finalsite will cooperate reasonably with LEA and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of Finalsite and/or delivery of Services to students and/or LEA, and shall provide reasonable access to Finalsite's facilities, staff, agents and LEA's Student Data and all records pertaining to Finalsite, LEA and delivery of Services to LEA, as reasonably necessary to fulfill such Security Audit requests. Failure to reasonably cooperate shall be deemed a material breach of the DPA. Finalsite may provide an independent third-party report or certification in place of allowing LEA to conduct such Security Audit.

5.3 **Data Security**. Finalsite agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. Finalsite shall adhere to any applicable law relating to data security. Finalsite shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth in Exhibit E. Additionally, Finalsite may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in Exhibit E. Finalsite shall provide, in Exhibit E to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.

5.4 **Data Breach**. To the extent required under Applicable Data Protection Laws, in the event that Finalsite becomes aware of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality, availability, or integrity of the Student Data maintained by Finalsite in violation of Applicable Data Protection Laws ("**Security Incident**"), Finalsite shall provide notification to LEA, to the extent required under Applicable Data Protection Laws, but in no event later than seventy-two (72) hours of confirmation of the Security Incident ("**Security Incident Notification**"), unless notification within this time limit would disrupt investigation of the Security Incident by law enforcement or by Finalsite. In such an event, notification shall be made within a reasonable time after the discovery of the Security Incident. Finalsite's obligation to report or respond to a Security Incident under this Section is not and will not be construed as an

acknowledgement by Finalsite of any fault or liability with respect to the Security Incident. Finalsite shall follow the following process:

5.4.1 Unless otherwise required by Applicable Data Protection Laws, the Security Incident Notification described above shall include, at a minimum, the following information to the extent known by Finalsite and as it becomes available:

5.4.1.1 The name and contact information of the reporting LEA subject to this section.

5.4.1.2 A list of the types of Student Data that were or are reasonably believed to have been the subject of a breach.

5.4.1.3 If the information is possible to determine at the time the notice is provided, then either (1) the date of the Security Incident, (2) the estimated date of the Security Incident, or (3) the date range within which the Security Incident occurred. The notification shall also include the date of the notice.

5.4.1.4 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

5.4.1.5 A general description of the Security Incident, if that information is possible to determine at the time the notice is provided.

5.4.2 Finalsite agrees to adhere to all federal and state requirements with respect to a Security Incident related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such Security Incident.

5.4.3 Finalsite 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 Security Incident involving 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.

5.4.4 To the extent that third party notice requirements under Applicable Data Protection Laws are triggered by the Security Incident, LEA shall provide notice on the facts surrounding the Security Incident to the affected students, parents or guardians. Finalsite will cooperate with LEA as to the timing and content of the notice.

5.4.5 In the event of a Security Incident originating from LEA's use of the Service, or otherwise a result of LEA's actions or inactions, Finalsite shall cooperate with LEA to the extent necessary to expeditiously secure Student Data, at LEA's cost.

ARTICLE 6 LIMITATION OF LIABILITY

6.1 **Limitation of Liability**. Each Party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and Finalsite, whether in contract, tort or under any other theory of liability, is subject to the 'Liability Limitation' section of the Agreement, and any reference in such section to the liability of a Party means the aggregate liability of that Party and all of its Affiliates under the Agreement and all DPAs together.

ARTICLE 7 MISCELLANEOUS

7.1 **Supplement State Terms**. To the extent Finalsite enters into the Agreement with an LEA located in one of the States identified within Exhibit F (Supplement State Terms) of this DPA, the terms specified in Exhibit F with respect to the applicable state apply in addition to the terms of this DPA. In the event of a conflict between this DPA's Standard Clauses and applicable Supplemental State Terms, the Supplemental State Terms will control.

7.2 **Termination**. In the event that either Party seeks to terminate this DPA, it may do so by mutual written consent so long as the Agreement has lapsed or has been terminated. Either party may terminate this DPA and any Agreement or contract if the other party breaches any terms of this DPA.

7.3 **Effect of Termination Survival**. If the Agreement is terminated, Finalsite shall destroy all of Student Data pursuant to Section 4.6.

7.4 **Entire Agreement**. This DPA and the 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.

7.5 **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.

7.6 **Governing Law; Venue and Jurisdiction**. THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF 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 LEA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.

7.7 **Successors Bound**. This DPA is and shall be binding upon the respective successors in interest to Finalsite 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 Finalsite sells, merges, or otherwise disposes of its business to a successor during the term of this DPA ("**Change of Control**"), Finalsite shall provide notice to LEA promptly after the closing date of such Change of Control. Such notice shall include assurances that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Agreement.

7.8 **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.

7.9 **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.

7.10 **Electronic Signature**. The Parties understand and agree that they have the right to execute this DPA through paper or through electronic signature technology, which is in compliance with applicable state and federal law governing electronic signatures. The Parties agree that to the extent they sign electronically, their electronic signature is the legally binding equivalent to their handwritten signature. Where they execute an electronic signature, it has the same validity and meaning as their handwritten signature. They will not, at any time in the future, repudiate the meaning of their electronic signature or claim that their electronic signature is not legally binding. They agree not to object to the admissibility of this DPA as an electronic record, or a paper copy of an electronic document, or a paper copy of a document bearing an electronic signature, on the grounds that it is an electronic record or electronic signature or that it is not in its original form or is not an original.

EXHIBIT A – DESCRIPTION OF SERVICES

Finalsite provides the following services through its platform or through consultancy ("**Services**"):

Details of the Services are listed in the Order and Statement of Work to which this DPA is incorporated by reference.

EXHIBIT B – SCHEDULE OF DATA

Category of Data	**Element**	**Check if used**
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 that are 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	✓
	Parent ID number (created to link parents to students)	✓
	First and/or Last	✓
Schedule	Student scheduled courses	
	Teacher names	
Special indicator	English Language Learner information	✓ (School Admin only)
	Low income status	✓(School Admin only)

	Medical alerts/health data	✓(School Admin only)
	Student disability information	✓(School Admin only)
	Specialized education services (IEP or 504)	✓(School Admin only)
	Living situations (Homeless/foster care)	✓(School Admin only)
	Other indicator information-Please specify:	
Student Contact information	Address	✓
	Email	✓
	Phone	✓
Student Identifiers	Local (school district) ID number	✓
	State ID number	✓
	Finalsite/App assigned student ID number	✓
	Student app username	✓
	Student app password	✓
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	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	✓
	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-Pease specify:	
Other	Please list each additional data element used, stored, or collected by your application:	
None	No Student Data collected at this time. Finalsite will immediately notify	

	LEA if this designation is no longer applicable.	

EXHIBIT C – DEFINITIONS

1.1 In this DPA, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

7.11 "**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

7.12 "**Applicable Data Protection Laws**" means United States federal and state privacy laws and regulations applicable to the Processing of Student Data pursuant to the Agreement, including 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), Protection of Pupil Rights Amendment ("PPRA") 20 U.S.C. 1232h.

7.13 "**Authorized Affiliate**" means an entity that (1) owns or controls, is owned or controlled by or is or under common control or ownership with LEA, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise, and (2) is permitted to use the Services provided by Finalsite pursuant to the Agreement between LEA and Finalsite.

7.14 "**De-Identified Data**" and "**De-Identification**" means records and information when all personally identifiable information has been removed or obscured, such that the remaining information does not reasonably identify a specific individual, including, 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.

7.15 "**Educational Records**" means records, files, documents, and other materials directly related to a student and maintained by LEA and its Authorized Affiliates, including, 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 result of evaluative tests, health data, disciplinary status, test protocols and individualized education programs.

7.16 **"LEA"** means the local educational agency, together with its Authorized Affiliates, that executed the Agreement, which determines the purposes and means of the Processing of Student Data. For the sake of clarity, references to LEA in this DPA concerns "Customer" as that term is defined under the Agreement.

7.17 "**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 has been stripped of all direct and indirect identifiers are not considered Personally Identifiable Information.

7.18 "**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.

7.19 "**Personal Identifiable Information**", "**Personal Information**" or "**PII**" means any information relating to an identified or identifiable natural person, that relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular natural person.

7.20 **"Processing"** means any operation or set of operations which is performed upon Personal Information, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

7.21 **"School Official"** means 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 redisclosure of Personally Identifiable Information from Education Records.

7.22 "**Services**" means the provision of maintenance and support services, consultancy or professional services and the provision of software as a service or any other services provided under the Agreement where Finalsite Processes Student Data.

7.23 "**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.

7.24 "**Student Data**" includes any data, whether gathered by Finalsite or provided by LEA or its users, students, students' parents/guardians, prospective students, and prospective 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 "Metadata." 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 shall not constitute that information that has been anonymized or De-Identified, or anonymous usage data regarding a student's use of Finalsite's services.

7.25 "**Subprocessor**" means any data processor (including any third party and any Finalsite Affiliate, but excluding an employee of Finalsite or any of its sub-contractors) appointed by or on behalf of Finalsite or any Finalsite Affiliate to Process Personal Data on behalf of LEA or Authorized Affiliates in connection with the Agreement.

7.26 "**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 website, 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 website based on the content of the webpage or in response to a student's response or request for information or feedback.

7.27 The word "**include**" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

EXHIBIT D – DIRECTIVE FOR DISPOSITION OF DATA

LEA directs Finalsite to dispose of Student Data obtained by Finalsite pursuant to the terms of the DPA between LEA and Finalsite. 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 Finalsite Date

EXHIBIT E – DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks

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 Finalsite.

Cybersecurity Frameworks

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

Security Coordinator. The name and contact information of each Party's designated representative for the purposes of matters relating to the security of Student Data received pursuant to the Agreement is set forth below:

1. Finalsite: Please contact our Security Committee at privacy@finalsite.com for any matters relating to the security of Student Data.

2. LEA's designated representative for matters relating to the security of Student Data is set forth on the signature page of the Order and Statement of Work.

EXHIBIT F – SUPPLEMENT STATE TERMS (CALIFORNIA)

1. The definition of "**Applicable Data Protection Law**" includes Student Online Personal Information Protection Act ("**SOPIPA**") at California Bus. & Prof. Code § 22584, and California Assembly Bill 1584 ("**AB 1584**") at California Education Code § 49073.1.

2. To the extent that LEA is subject to the California Consumer Privacy Act of 2018 (CCPA) and/or the California Privacy Rights Act of 2020 (CPRA), "**Student Data**" includes any information relating to an identified or identifiable natural person that relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular natural person.

3. **Modification to Section 5.7 of the DPA**. Section 5.7 of the DPA (Advertising Limitations) is amended by deleting the stricken text as follows:

Finalsite 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 Finalsite 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.

EXHIBIT F– SUPPLEMENT STATE TERMS (ILLINOIS)

1. **Compliance with Illinois Privacy Laws.** In performing its obligations under the Agreement, Finalsite shall comply with all Illinois laws and regulations pertaining to student data privacy, confidentiality, and maintenance, including but not limited to the Illinois School Student Records Act ("ISSRA"), 105 ILCS 10/, Mental Health and Developmental Disabilities Confidentiality Act ("MHDDCA"), 740 ILCS llO/, Student Online Personal Protection Act ("SOPPA"), 105 ILCS 85/, Identity Protection Act ("IPA"), 5 ILCS 179/, and Personal Information Protection Act ("PIPA"), 815 ILCS 530/, and Local Records Act ("LRA"), 50 ILCS 205/.

2. **Definition of "Student Data."** In addition to the definition set forth in **Exhibit C,** Student Data includes any and all information concerning a student by which a student may be individually identified under applicable Illinois law and regulations, including but not limited to (a) "covered information," as defined in Section 5 of SOPPA (105 ILCS 85/5), (b) "school student records" as that term is defined in Section 2 of ISSRA (105 ILCS 10/2(d)) (c) "records" as that term is defined under Section 110/2 of the MHDDCA (740 ILCS 110/2), and (d) "personal information" as defined in Section 530/5 of PIPA.

3. **School Official Designation.** Pursuant to Article 1, Section 1.1 of the DPA, and in accordance with FERPA, ISSRA and SOPPA, in performing its obligations under the DPA, Finalsite is acting as a school official with legitimate educational interest; is performing an institutional service or function for which LEA would otherwise use its own employees; is under the direct control of LEA with respect to the use and maintenance of Student Data; and is using Student Data only for an authorized purpose and in furtherance of such legitimate educational interest.

4. **Limitations on Re-Disclosure.** Finalsite shall not re-disclose Student Data to any other party or affiliate without the express written permission of LEA or pursuant to court order, unless such disclosure is otherwise permitted under SOPPA, ISSRA, FERPA, and MHDDCA. Finalsite will not sell or rent Student Data. In the event another party, including law enforcement or a government entity, contacts Finalsite with a request or subpoena for Student Data in the possession of Finalsite, Finalsite shall redirect the other party to seek the data directly from LEA. In the event Finalsite is compelled to produce Student Data to another party in compliance with a court order, Finalsite shall notify LEA at least five (5) school days in advance of the court ordered disclosure and, upon request, provide LEA with a copy of the court order requiring such disclosure.

5. **Notices.** Any notice delivered pursuant to the DPA shall be deemed effective, as applicable, upon receipt as evidenced by the date of transmission indicated on the transmission material, if by email; or four (4) days after mailing, if by first-class mail, postage prepaid.

6. **Parent Right to Access and Challenge Student Data.** LEA shall establish reasonable procedures pursuant to which a parent. as that term is defined in 105 ILCS 10/2(g), may inspect and/or copy Student Data and/or challenge the accuracy, relevance or propriety of Student Data, pursuant to Sections 5 and 7 of ISSRA (105 ILCS 10/5; 105 ILCS 10/7) and Section 33 of SOPPA (105 ILCS 85/33). Finalsite shall respond to any request by LEA for Student Data in the possession of Finalsite when Finalsite's cooperation is required to afford a parent an opportunity to inspect and/or copy the Student Data, no later than 5 business days from the date of the request. In the event that a parent contacts Finalsite directly to inspect and/or copy Student Data, Finalsite shall refer the parent to LEA. which shall follow the necessary and proper procedures regarding the requested Student Data.

7. **Corrections to Factual Inaccuracies.** In the event that LEA determines that Finalsite is maintaining

Student Data that contains a factual inaccuracy, and Finalsite's cooperation is required in order to make a correction, LEA shall notify Finalsite of the factual inaccuracy and the correction to be made. No later than 90 calendar days after receiving the notice of the factual inaccuracy, Finalsite shall correct the factual inaccuracy and shall provide written confirmation of the correction to LEA.

8. **Security Standards.** Finalsite shall implement and maintain commercially reasonable security procedures and practices that otherwise meet or exceed industry standards designed to protect Student Data from unauthorized access, destruction, use, modification, or disclosure, including but not limited to the Security Incident. For purposes of the DPA and this Exhibit G, "Security Incident" does not include the good faith acquisition of Student Data by an employee or agent of Finalsite or LEA for a legitimate educational or administrative purpose of Finalsite or LEA, so long as the Student Data is used solely for purposes permitted by SOPPA and other applicable law, and so long as the Student Data is restricted from further unauthorized disclosure.

9. **Security Incident Notification.** In addition to the information enumerated in Article 5, Section 5.4.1 of the DPA Standard Clauses, any Security Incident Notification provided by Finalsite to LEA shall include:

    a. A list of the students whose Student Data was involved in or is reasonably believed to have been involved in the breach, if known; and

    b. The name and contact information for an employee of Finalsite whom parents may contact to inquire about the breach.

10. **Reimbursement of Expenses Associated with Security Incident.** In the event of a Security Incident that is attributable to Finalsite, subject to the "Liability Limit" section of the Master Terms and where Finalsite and its Affiliates' aggregate liability does not exceed the amount specified in the Agreement, Finalsite shall reimburse and indemnify LEA for any and all costs and expenses that LEA incurs in investigating and remediating the Security Incident, including but not limited to costs and expenses associated with:

    a. Providing notification to the parents of those students whose Student Data was compromised and regulatory agencies or other entities as required by law or contract;

    b. Providing credit monitoring to those students whose Student Data was exposed in a manner during the Security Incident that a reasonable person would believe may impact the student's credit or financial security;

    c. Legal fees, audit costs, fines, and any other fees or damages imposed against LEA as a result of the Security Incident; and

    d. Providing any other notifications or fulfilling any other requirements adopted by the Illinois State Board of Education or under other State or federal laws.

11. **Transfer or Deletion of Student Data.** Finalsite shall review, on an annual basis, whether the Student Data it has received pursuant to the DPA continues to be needed for the purpose(s) of the Agreement and this DPA. If any of the Student Data is no longer needed for purposes of the Agreement and this DPA, Finalsite will provide written notice to LEA as to what Student Data is no longer needed. Finalsite will delete or transfer Student Data in readable form to LEA as directed by LEA (which may be

effectuated through **Exhibit D** of the DPA) within 30 calendar days if LEA requests deletion or transfer of the Student Data and shall provide written confirmation to LEA of such deletion or transfer. Upon termination of the Service Agreement between Finalsite and LEA, Finalsite shall conduct a final review of Student Data within 60 calendar days. If LEA receives a request from a parent, as that term is defined in 105 ILCS 10/2(g), that Student Data being held by Finalsite be deleted, LEA shall determine whether the requested deletion would violate State and/or federal records laws. In the event such deletion would not violate State or federal records laws, LEA shall forward the request for deletion to Finalsite. Finalsite shall comply with the request and delete the Student Data within a reasonable time period after receiving the request. Any provision of Student Data to LEA from Finalsite shall be transmitted in a format readable by LEA.

12. **Public Posting of DPA.** Pursuant to SOPPA, LEA shall publish on its website a copy of the DPA between Finalsite and LEA. including this **Exhibit G**.

13. **Subcontractors.** By no later than (5) business days after the date of execution of the DPA, Finalsite shall provide LEA with a list of any subcontractors to whom Student Data may be disclosed or a link to a page on Finalsite's website that clearly lists any and all subcontractors to whom Student Data may be disclosed. This list shall, at a minimum, be updated and provided to LEA by the beginning of each fiscal year (July 1) and at the beginning of each calendar year (January 1).

14. **DPA Term.** Paragraph 4 on page 1 of the DPA setting a three-year term for the DPA shall be deleted, and the following shall be inserted in lieu thereof: "This DPA shall be effective upon the date of signature by Finalsite and LEA. and shall remain in effect as between Finalsite and LEA 1) for so long as the Services are being provided to LEA or 2) until the DPA is terminated pursuant to Section 15 of this Exhibit G, whichever comes first. "

15. **Termination.** Article 7, Section 7.2 shall be deleted, and the following shall be inserted in lieu thereof: "In the event either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Agreement has lapsed or been terminated. One party may terminate this DPA upon a material breach of this DPA by the other party. Upon termination of the DPA, the Agreement shall terminate.'

16. **Privacy Policy.** Finalsite must publicly disclose material information about its collection, use, and disclosure of Student Data, including, but not limited to, publishing a terms of service agreement, privacy policy, or similar document.

17. **Minimum Data Necessary Shared.** Finalsite attests that the Student Data request by Finalsite from LEA in order for LEA to access Finalsite's products and/or services is limited to the Student Data that is adequate, relevant, and limited to what is necessary in relation to the K-12 school purposes for which it is processed.

18. **Student and Parent Access.** Access by students or parents/guardians to Finalsite's programs or services governed by the DPA or to any Student Data stored by Finalsite shall not be conditioned upon agreement by the parents/guardians to waive any of the student data confidentiality restrictions or a lessening of any of the confidentiality or privacy requirements contained in this DPA.

19. **Data Storage.** Finalsite shall store all Student Data shared under the DPA within the United States.

20. **Exhibits A and B.** The Services described in **Exhibit A** and the Schedule of Data in **Exhibit B** to the DPA

satisfy the requirements in SOPPA to include a statement of the product or service being provided to the school by Finalsite and a listing of the categories or types of covered information to be provided to Finalsite, respectively.

EXHIBIT F– SUPPLEMENT STATE TERMS (MASSACHUSETTS)

1. The definition of "Applicable Data Protection Law" includes 603 C.M.R. 23.00, Massachusetts General Law, Chapter 71, Sections 34D to 34H and 603 CMR 28.00.

2. All employees of Finalsite who will have direct contact with students shall pass criminal background checks.

EXHIBIT F – SUPPLEMENT STATE TERMS (NEW YORK)

2 The definition of "**Applicable Data Protection Law**" includes New York State Education Law 2-d.

3 Finalsite agrees that it will comply in all material respects with those provisions of the "LEA's Parent's Bill of Rights for Data Security and Privacy" ("**Parents Bill of Rights**"), a copy of which is attached below that is applicable to Finalsite.

4 The detailed security programs and measures in Exhibit D shall include, but not limited to:

4.1 **Employee Training**. Finalsite shall provide periodic security training to those of its employees who operate or have access to the Services.

4.2 **Security Technology**. When the Service is accessed using a supported web browser, Secure Socket Layer ("SSL"), or equivalent technology shall be employed to protect Student Data from unauthorized access. The security measures employed shall include server authentication and data encryption at rest and in transit. Finalsite shall host Student Data pursuant to the Agreement in an environment using a firewall that is maintained according to industry standards.

4.3 In the event of a Security Incident involving Student Data, as defined in Section 6.4, LEA shall (a) upon notification by Finalsite, report the Security Incident to the Chief Privacy Officer, who is appointed by the New York State Education Department; and (b) notify the parent or eligible student of the unauthorized release of Student Data that includes Personally Identifiable Information from the student records of such student in the most expedient way possible and without unreasonable delay. In the case of notification to a parent or eligible student, due to a Security Incident involving Student Data by Finalsite, or its Subprocessors or assignees, and such Security Incident is not originating from LEA's use of the Service or otherwise a result of LEA's actions or inactions, Finalsite, if requested by LEA and provided that Finalsite has not previously notified the affected parties, shall promptly reimburse LEA for the full cost of such notification, as required by Education Law §2-d(6)(c).

PARENTS BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

Pursuant to Section 2-d of the New York State Education Law ("Education Law §2-d"), parents and eligible students are entitled to certain protections regarding confidential student information. Customer, as defined in the Agreement is committed to safeguarding personally identifiable information from unauthorized access or disclosure as set forth below: Any terms not defined herein, shall have the meaning set forth in Education Law §2-d and if not defined in Education Law §2-d, in the Data Processing Addendum (DPA) to which this document is an Exhibit.

1. A student's personally identifiable information cannot be sold or released for any commercial purposes;

2. Parents have the right to inspect and review the complete contents of their child's education record maintained by the Customer;

3. State and federal laws protect the confidentiality of personally identifiable information. The Customer is committed to implementing safeguards associated with industry standards and best practices under state and federal laws protecting the confidentiality of personally identifiable information, including but not limited to, encryption, firewalls, and password protection when data is stored or transferred;

4. A complete list of all Student Data elements collected by the State is available for public review at http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx or by writing to the NYS Education Department, Information & Reporting Services, Room 863 EBA, 89 Washington Avenue, Albany, NY 12234;

5. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to the Customer;

6. The Customer has entered into contracts with certain third-party contractors/consultants who have received Student Data and/or teacher data and/or principal data. These contracts will include the following supplemental information:

    a. The exclusive purpose(s) for which the Student Data will be used;

    b. The commencement and termination dates of each such contract;

    c. A description of how the Student Data will be disposed by the contractor upon expiration of the contract;

    d. If and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the Student Data or teacher or principal data that is collected; and

    e. The data storage and security measures undertaken for Student Data or teacher or principal data, including whether such data will be encrypted.

7. Agreements with third party contractors/consultants will ensure that the subcontractors, persons or entities that the third party contractor will share the Student Data or teacher or principal data with, if any, will abide by data protection and security requirements.

EXHIBIT F– SUPPLEMENT STATE TERMS (OREGON)

1. The definition of "Applicable Data Protection Law" includes applicable Oregon laws and regulations, including SB 187 (2015), Oregon Student Information Protection Act ("OSIPA"), Or. Rev. Stat. § 646.607 – 646.652; Or. Rev. Stat. § 326.565, et seq. (Student Records), and other applicable state privacy laws and regulations.

EXHIBIT F– SUPPLEMENT STATE TERMS (TEXAS)

1. **Covered Data.** All instances of "Student Data" should be replaced with "LEA Data." The protections provided within this DPA extend to all data provided to or collected by Finalsite.

2. **Compliance with Texas Privacy Laws and Regulations.** In performing their respective obligations under the Agreement, LEA and Finalsite shall comply with all Texas laws and regulations pertaining to data privacy and confidentiality applicable to LEA Data, including but not limited to the Texas Education Code Chapter 32, and Texas Government Code Chapter 560.

3. **Modification to Section 6.4 of the DPA.** Section 6.4 of the DPA (Data Breach) is amended with the following additions:

   6.4.6 For purposes of defining an unauthorized disclosure or security breach, this definition specifically includes meanings assigned by Texas law, including applicable provisions in the Texas Education Code and Texas Business and Commerce Code.
   6.4.7 LEA may immediately terminate the Agreement if LEA determines Finalsite has breached a material term of this DPA.
   6.4.8 Finalsite's obligations shall survive termination of this DPA and Agreement until all Student Data has been returned and/or securely destroyed.

4. **Modification to Section 8.4 of the DPA.** Section 8.4 of the DPA (Entire Agreement) is amended as follows:

   Entire Agreement. This DPA and the Agreement constitutes 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. **Reimbursement of Expenses Associated with Security Breach.** In the event of a Security Breach that is attributable to Finalsite, subject to the "Liability Limitation" section of the Master Terms and where Finalsite and its Affiliates' aggregate liability does not exceed the amount specified in the Agreement, Finalsite shall reimburse and indemnify LEA for any and all costs and expenses that LEA incurs in investigating and remediating the Security Breach, including but not limited to costs and expenses associated with:

a. Providing notification to the employees or parents of those students whose Student Data was compromised and regulatory agencies or other entities as required by law or contract;
b. Providing credit monitoring to those employees or students whose Student Data was exposed in a manner during the Security Breach that a reasonable person would believe may impact the employee's or student's credit or financial security;
c. Legal fees, audit costs, fines, and any other fees or damages imposed against LEA as a result of the security breach; and
d. Providing any other notifications or fulfilling any other requirements adopted by the Texas State Board of Education, Texas Education Agency, or under other State or federal laws.

EXHIBIT F – SUPPLEMENT STATE TERMS (WASHINGTON)

1. The definition of "**Applicable Data Protection Law**" includes applicable Washington laws and regulations, such as the Student User Privacy in Education Rights 28.A.604 et seq. and RCW 42.56.590.

2. **Modification to Section 5.2 of the DPA**. Section 5.2 of the DPA is hereby amended to read as follows:

   Authorized Use: The Student Data shared pursuant to the Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in Exhibit A or stated in the Agreement and/or otherwise authorized under the statutes referred to herein this DPA, unless Processing is required by Applicable Data Protection Laws to which Finalsite is subject, in which case Finalsite shall, to the extent permitted by Applicable Data Protection Laws, inform LEA of that legal requirement before the relevant Processing of that Student Data. Finalsite may use or disclose data to:

   (a) Protect the security or integrity of its website, mobile application or online service.

   (b) Ensure legal or regulatory compliance or to take precautions against liability.

   (c) Respond to or participate in the judicial process.

   (d) Protect the safety of users or others on the website, mobile application or online service.

   (e) Investigate a matter related to public safety.

   In undertaking the activities specified in subsections (a) through (e) above, Finalsite shall adhere to all applicable data protections contained in this DPA, as well as Federal and Washington State law.

3. **Modification to Section 5.7 of the DPA.** Section 5.7 is hereby amended to add the following language:

   (iv) providing recommendations for school, educational, or employment purposes within a school service without the response being determined in whole or in part or other consideration from a third party.