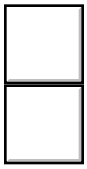

(as of October 1, 2021)

Finalsite Master Terms and Conditions for Services

THESE MASTER TERMS AND CONDITIONS (“MASTER TERMS”) APPLY TO ALL SERVICES MADE AVAILABLE BY ACTIVE INTERNET TECHNOLOGIES, LLC, dba FINALSITE, A CONNECTICUT CORPORATION HAVING A PRINCIPAL PLACE OF BUSINESS AT 655 WINDING BROOK DRIVE, GLASTONBURY, CONNECTICUT 06033 AND ITS AFFILIATES (“FINALSITE”) FOR THE CUSTOMER (FINALSITE AND CUSTOMER SOMETIMES COLLECTIVELY REFERRED TO AS THE “PARTIES”). THE “CUSTOMER” IS AN ENTITY WHICH ENTERS INTO AN ORDER WITH FINALSITE PURSUANT TO THESE MASTER TERMS. EACH ORDER EXECUTED BY THE PARTIES FORMS A SEPARATE CONTRACT BETWEEN THE PARTIES WHICH INCORPORATES AND IS GOVERNED BY THESE MASTER TERMS.

1. Ordering Services.

1.01 Customer may purchase from Finalsite the right to use one or more software-as-a-service (“SaaS”) applications and/or modules (collectively, “SaaS Services”) which will be

(collectively, "Support Services") (SaaS Services, Hosting Services, Deployment Services, Professional Services and Support Services sometimes collectively referred to in these Master Terms as "Services"). In each instance in which Customer wishes to purchase Services from Finalsite, the Parties shall enter into a mutually agreed order document describing the particular Services ordered and any special conditions or terms applicable thereto (each an "Order"). Customer shall only have the right to receive those Services specified in an applicable Order. In addition, the Parties may enter into a Statement of Work ("SOW") which is mutually agreed to by the Parties to further describe certain Services. In order to be effective, a SOW shall reference the applicable Order and either be incorporated into to the Order or separately executed by both Parties. When mutually agreed and signed by duly-authorized representatives of each Party, each Order shall be and hereby is deemed to be governed by these Master Terms. These Master Terms (as may be amended or supplemented from time to time), together with each fully executed Order and SOW, forms the contract between Finalsite and Customer (collectively, the "Agreement"). In the event of any conflict between the terms and conditions of these Master Terms and the terms and conditions of any Order, the terms and conditions of the Order shall control with respect to such Order.

2. Access to SaaS Services/Restrictions.

2.01 Subject to the terms and conditions of this Agreement, upon entering into an Order therefor, Finalsite shall make the relevant SaaS Services immediately available to Customer on the Effective Date of the applicable Order for use by Customer and its Authorized Users in accordance with the terms of this Agreement and Finalsite's Privacy Policy set forth at finalsite.com/privacy. Additional usage limitations or restrictions may be imposed on Customer's use of the SaaS Services in the relevant Order, including limitations on bandwidth and storage. Due to the nature of a SaaS delivery model, the SaaS Services to which the Customer is provided access will be the then-current version of such SaaS Services which is made available by Finalsite for its customers generally.

2.02 Customer and its employees, faculty, administrators, students, parents of students, alumni and/or third party service providers who are authorized by Customer to use the

SaaS Services on Customer's behalf (collectively, "Authorized Users") may access the SaaS Services, along with applicable content displayed by Customer through the use thereof, over the internet via Finalsite's hosted website solely in support of Customer's operations and within the scope of Customer's permitted use of the SaaS Services. With respect to public-facing content which the SaaS Services are designed to display, Authorized Users include individuals who access the screen displays of the SaaS Services on a remote, web-enabled basis in order to view the content which Customer has chosen to display to the public. Customer shall be fully responsible for any acts or omissions of its Authorized Users, including any unauthorized use of the SaaS Services or other breach of this Agreement. All rights not expressly granted to Customer in this Agreement are reserved to Finalsite and its licensors.

2.03 Except as expressly set forth in these Master Terms or an Order, Customer shall not, and shall not permit its Authorized Users or other third parties to (i) use, copy, sell, assign, sublicense, convey or otherwise transfer, all or any portion of the SaaS Services; (ii) decompile, disassemble or otherwise reverse engineer the SaaS Services or any portion thereof; (iii) modify, translate or create any derivative works based on the SaaS Services; (iv) remove or alter any copyright notices, trademarks or other proprietary rights notices affixed to or contained within the SaaS Services (v) resell or sublicense the SaaS Services or use the SaaS Services to provide any services on behalf of, or for the benefit of itself or any third parties; or (vi) violate or cause the violation of any law, regulation, order, decree or judgment in connection with the use of any Services or any content or data utilized therewith.

3. Hosting Services.

Finalsite will provide Hosting Services and Support Services in accordance with the Service Level Agreement ("SLA") attached as Schedule 1 to these Master Terms.

4. Deployment and Professional Services.

4.01 Certain Deployment Services and other Professional Services may require that the Parties agree to a SOW, which may include a timetable for delivery and other

assumptions. Any timetable set forth in a SOW, Order or other project document is a good faith estimate which is dependent on, among other factors, Customer's provision of appropriate information, cooperation, assistance, and tasks, including those items which may be identified as the responsibility of Customer in the SOW.

4.02 Subject to Section 7 below, Customer shall provide Finalsite access to Customer's logos and trademarks and other content as may be necessary Finalsite to perform the Deployment Services and other Services described in an Order.

4.03 Finalsite will provide all Professional Services and Deployment Services in a professional and workmanlike manner and in accordance in all material respects with any and all descriptions or requirements set forth in an applicable SOW. If deliverables are provided as part of the Deployment Services and/or the Professional Services and those deliverables do not conform in all material respects to any applicable specifications and other requirements which are described in the applicable Order or SOW, Customer shall give Finalsite written notification of the deficiency or non-conformance within thirty (30) days after delivery of such Services. Finalsite then shall, within thirty (30) days of receipt of such written notification, use commercially reasonable efforts to correct the deficiency. Customer shall provide such support and assistance as reasonably requested by Finalsite to discover the cause or a cure for the reported deficiency or non-conformance.

5. Support.

5.01 Finalsite shall provide Customer Support Services in accordance with Finalsite's then-current standard support policies and practices as and when made available to customers generally. Finalsite supports Customer's browser access to the SaaS Services utilizing the then-current version and one prior version of Internet Explorer, Safari, Chrome or Firefox.

5.02 Certain Support Services are accessible through the "Help" section located in Customer's interface to the SaaS Services. Certain other Support Services (such as expedited or "priority" support) may be purchased by Customer under an Order, and, in such event, the terms and conditions of such Support Services, and associated fees, shall

be as described in the applicable Order.

6. Third Party Technology.

6.01 Finalsite may utilize certain software or other technology of third parties (collectively, "Third Party Technology") in connection with its provision of the SaaS Services and/or the SaaS Services may enable Customer to interact with and/or utilize certain Third Party Technology. For example, Third Party Technology may include third party materials such as online chat services, site translation services, accessibility overlay solutions, font and typography services, and any web service, website, social media platform or online library that enables functionality within a webpage displayed by the SaaS Services. Except as otherwise expressly provided below, Customer is solely responsible and liable for Customer's access to or use of any Third Party Technology. To the extent that Finalsite incorporates or embeds Third Party Technology into the SaaS Services such that it becomes part of the functionality of the SaaS Services, then such Third Party Technology shall be included in the SaaS Services provided by Finalsite in accordance with the terms of this Agreement.

6.02 Providers of Third Party Technology are approved Subcontractors of Finalsite under the Finalsite Data Processing Addendum, to the extent applicable to Processing under these Mater Terms, as described in Schedule 2.

7. Ownership.

7.01 Customer shall own: (a) all data and content that Customer and its Authorized Users input, post, submit, or otherwise provide to Finalsite while utilizing the SaaS Services under this Agreement (where "content" includes text, images, and sounds); and (b) Customer's logos and trademarks ((a) and (b), collectively "Customer Materials"). Customer shall be solely responsible and liable for the content, accuracy or completeness of all Customer Materials (including monitoring the content posted on the website), and for any infringement by any Customer Materials of third party intellectual property rights. For clarity, Customer Materials includes Customer's Personal Information and Student Data (as such terms are defined in these Master Terms).

7.02 Finalsite shall not use Customer Materials except: (a) as requested or permitted by Customer; (b) in connection with providing, facilitating or supporting the Services or otherwise exercising rights or performing obligations under this Agreement (including, for example, by addressing technical and other issues related to the Services); or (c) to the extent required, or permitted, by applicable laws or regulations; and/or (d) as otherwise permitted under this Agreement.

7.03 Finalsite and its licensors own all right, title, and interest in and to the SaaS Services (including the underlying software and all application program interfaces ("API's") provided or made available by Finalsite) and all documentation, materials, work product and deliverables resulting from or related to the Services (including in each case all enhancements, modifications, updates, upgrades and derivative works thereof and all intellectual property rights in any of the foregoing). Any enhancements, modifications, derivative works or any other intellectual property created directly or indirectly using or referring to the SaaS Services or components thereof, whether created solely by Customer or a third party on behalf of Customer, or jointly by Customer and Finalsite or a third party on either party's behalf, belong exclusively to Finalsite, and Customer hereby irrevocably assigns all rights therein (including without limitation, all patent, copyright, trademark, trade secret and moral rights) to Finalsite. In the event that Customer or any of its Authorized Users submit any ideas, suggestions, proposed enhancements, or other feedback relating to the SaaS Services (collectively, "Feedback"), Finalsite shall own all such Feedback without compensation to Customer or its Authorized Users and Customer hereby irrevocably assigns all rights in such Feedback to Finalsite.

8. Security and Data Privacy.

8.01 In connection with use of the Services set forth in an Order, Customer or an Authorized User may from time to time provide Finalsite with certain personally identifiable information of Customer's students, prospective students, parents of students, faculty, administrators, employees and/or Authorized Users that is protected by various laws and regulations ("Personal Information"). Personal Information may include Student Data to the extent it meets the definition set forth in Schedule 2 to these Master Terms. Customer

represents and warrants that it has the right to provide such Personal Information to Finalsite.

8.02 Without limiting the provisions set forth in Schedule 2 or Customer's obligations under these Master Terms, Finalsite shall maintain reasonable and appropriate security measures designed to protect Personal Information from unauthorized access, destruction, use, modification and disclosure. Finalsite shall not use or disclose Personal Information, except for the purposes for which it is permitted to use or disclose Customer Materials under these Master Terms. Similarly, Customer shall comply with all laws and regulatory requirements governing Personal Information which are applicable to Customer.

8.03 Customer shall maintain reasonable and appropriate security measures to protect the confidentiality and integrity of its account IDs, passwords, and interaction with the Services. Customer shall be responsible for all activities that occur under its account, regardless of whether the activities are authorized by the Customer or undertaken by Customer, its employees and other representatives or Authorized Users and Finalsite is not responsible for unauthorized access to your account.

9. Additional Data Privacy Terms. The applicable privacy terms set forth in Schedule 2 are part of these Master Terms.

10. Consent to Use/Transfer

10.01 Customer represents and warrants that at all times during the Term, it has obtained all consents necessary for Finalsite to access and use the Customer Materials for purposes of providing the Services, including those consents related to the collection, use, maintenance and transfer of Personal Information and Student Data (as defined in Schedule 2) from students in compliance with applicable law and regulatory requirements (including the Children's Online Privacy Protection Act, as amended). Finalsite may rely on this Agreement as Customer's representation that all necessary consents have been obtained and Finalsite shall not be required to independently verify such fact or compliance by Customer with applicable law with respect thereto.

10.02 Customer further represents and warrants that the use of Personal Information and other Customer Materials by Finalsite, in accordance with the terms of the Agreement, does not and will not violate any applicable law or regulatory requirements, or result in the breach of any covenant or obligation that Customer has to any person or entity. Customer acknowledges that Finalsite has no responsibility to review or monitor any Customer Materials, including reviewing or determining the legality, accuracy or completeness of Customer Materials. Finalsite, however, reserves the right to take any action with respect to the Services that Finalsite deems necessary or appropriate in its sole discretion if Finalsite reasonably believes Customer's use of the Services could violate applicable law or regulatory requirements, create liability for Finalsite, its affiliates and/or its suppliers, or could otherwise compromise or disrupt services provided to other customers.

10.03 Customer acknowledges and agrees that, in the course of Finalsite providing Services hereunder, Finalsite may provide access to Customer Materials to employees, affiliates, subcontractors and third party service providers ("Representatives") who have a legitimate need to access such information in order to provide their services to Finalsite as part of Finalsite's provision of Services to Customer. By way of example, Representatives include third parties who provide back-up, hosting, support and business recovery services. Representatives shall be required to maintain the confidentiality of all Confidential Information of Customer.

10.04 Customer agrees that Finalsite may collect, use and disclose data which is generated, collected or derived in connection with the use of the SaaS Services by Customer and its Authorized Users, including data derived from the Customer Materials to: (a) determine usage trends, (b) conduct research and development (including enhancing its products and services), (c) collect and analyze cookies and other metadata, (d) create analytics and (e) for other business purposes; provided that such data shall be de-identified (such that it will not identify Customer or any natural person) and aggregated (collectively, "De-Identified Data"). Subject to the above conditions, Finalsite shall own all De-Identified Data.

11. Customer Responsibilities.

11.01 In addition to its other responsibilities as set forth in this Agreement, Customer is solely responsible for and assumes all liability relating to (i) decisions about Customer's computer and communications systems needed to access the SaaS Services; (ii) all purchases of any necessary hardware, software, services or licenses required by Customer to access and use the SaaS Services as contemplated in this Agreement; (iii) Customer's procedures and criteria, including any claim by an applicant, student, parent or employee arising from Customer's procedures or criteria and any violation of any applicable statutory or regulatory requirements resulting from implementation of Customer's procedures and criteria; and (iv) provision and maintenance of all domains and URLs used by Customer and its Authorized Users to access the Services.

11.02 Customer and its Authorized Users shall comply with all applicable law and regulatory requirements in their respective execution, delivery and performance of this Agreement and access to and use of the Services.

11.03 Customer represents and warrants, and shall ensure that it and all Authorized Users shall not: (i) use the Services, in whole or in part, to store, initiate or transmit material (including Customer Materials) that is infringing, libelous, defamatory, abusive, harmful to minors, designed to cause annoyance, inconvenience or distress to any person; comprises unsolicited marketing (i. e. spam), in violation of third-party privacy or property rights, or otherwise tortious or in violation of applicable law: (ii) interfere with, unreasonably burden, or disrupt the integrity or performance of the Services or third-party data or content contained therein; (iii) attempt to gain unauthorized access to the Services or its related systems or networks; (iv) provide the Services to third parties who are not Authorized Users, including, by resale, license, loan or lease; and, (v) without Finalsite's prior written consent, imply or state, directly or indirectly, that Customer is affiliated with or endorsed by Finalsite; or, publicize the existence of the Agreement, or any of its terms. Customer will use best efforts to prevent and/or block any prohibited use, and will cooperate with Finalsite to prevent or cease such use from continuing. Customer will notify Finalsite immediately in writing, if it knows or has reason to know that that the Services are being used in violation of the Agreement or applicable law, describing such violation(s), and the basis for such knowledge, and shall be solely responsible and liable, and shall ensure that Finalsite, its

officers, directors, representatives and its affiliates are not responsible or liable, for such violative use.

12. Term of the Agreement/Orders.

This Agreement shall become effective on the effective date of the first Order entered into by Customer and Finalsite and shall continue through the termination date of all Orders hereunder (the "Term"), unless terminated earlier in accordance with the provisions of this Agreement. The term of any Order shall be stated in the Order, provided however that unless otherwise provided in any Order, the term of each Order shall automatically renew for successive terms of equal duration to the initial term stated therein unless either Party provides written notice of its intent not to renew at least thirty (30) days prior to the expiration of the then-current term.

13. Termination

13.01 In the event either party defaults in any obligation in this Agreement or any Order, the non-defaulting Party shall give written notice of such default. If the Party in default has not cured the default within thirty (30) days of receipt of the notice, the non-defaulting Party may terminate this Agreement by delivering written notice thereof to the defaulting Party.

13.02 Either Party may terminate this Agreement, effective immediately upon written notice, in the event that the other party: (i) makes a general assignment for the benefit of creditors; (ii) institutes proceedings seeking relief or reorganization under any laws relating to bankruptcy or insolvency or (iii) has a court of competent jurisdiction appoint a receiver, liquidator or trustee over all or substantially all of such party's property or provides for the liquidation of such Party's property or business affairs.

13.03 Either party may terminate this Agreement upon written notice at any time when there are no Orders then in effect.

13.04 Customer shall have the right to terminate an Order for convenience if it first meets all of the following conditions: (i) it must provide Finalsite with at least sixty (60) days' prior written notice of such termination of the applicable Order, including the effective date of

termination; (ii) it must pay Finalsite, on or before the effective date of termination, all fees and expenses which are due for Services provided through the effective date of such termination; and (iii) it must pay Finalsite, on or before the effective date of termination, an amount equal to the full amount of the fees owed to Finalsite for all periods from the effective date of termination through the end of the then-current Term of the terminated Order.

13.05 Customer commits that it has sufficient available funds to pay for the Services purchased under each Order through at least the end of the then-current fiscal year. If Customer is a public school district or other governmental entity and for any fiscal year thereafter during which an Order is in effect, sufficient funds are not appropriated by Customer's public funding body to pay in full the fees due under such Order for that fiscal year, then Customer shall have the right to terminate the relevant Order by providing Finalsite written notice of termination at least ninety (90) days prior to the first day of the fiscal year for which sufficient funds will not be available and by paying Finalsite in full for all fees and expenses due through the end of the then-current fiscal year. Customer agrees that the termination rights set forth in this Section 13.05 will not apply if any funds are appropriated to it for the acquisition, retention or operation of software or other services substantially similar to the Services provided by Finalsite hereunder. Customer agrees to use its best efforts to obtain and maintain sufficient funds to make all payments due hereunder and commits that it will only utilize this provision in the event that, despite its good faith best efforts to continue to fund all Order under this Agreement, such funds were withdrawn by its funding body.

13.06 Termination of this Agreement or any Order shall terminate all Services provided by Finalsite thereunder, and Customer and its Authorized Users shall cease all use of the applicable Services on or before the effective date of termination or expiration. The due dates of all payments owed by Customer to Finalsite under this Agreement shall become due on the effective date of termination or expiration.

14. Subcontractors.

Finalsite may utilize third party subcontractors and/or service providers to perform, or support performance of, any Services under this Agreement in its sole discretion, subject to the terms of Schedule 2 and Finalsite's standard Data Processing Addendum to the extent applicable, and applicable law. In such event, Finalsite shall not be relieved from its obligations under this Agreement. Customer hereby provides its general consent to Finalsite to such subcontracting.

15. Fees and Expenses

15.01 All fees and expenses payable by Customer shall be payable in U.S. Dollars in the amounts and on such payment dates as described in the applicable Order. Customer may ACH or wire payments or pay via check. If Customer elects to pay via check, the check must be drawn on a U.S. bank. Finalsite may increase fees effective on the annual anniversary date of each Order by providing at least sixty (60) days' advance written notice to Customer of the increase, provided that any such increase shall not exceed the greater of seven percent (7%) of the fees due for the immediately preceding year or the most recently-measured annual increase in the U.S. Consumer Price Index for the immediately preceding annual period. All amounts payable by Customer under this Agreement will be paid to Finalsite without setoff or counterclaim, and without any deduction or withholding.

15.02 In addition to the fees for Services, Customer shall reimburse Finalsite for all agreed out-of-pocket expenses incurred by Finalsite in connection with provision of the Services at actual cost within thirty (30) days of the invoice date following completion of the relevant Services.

15.03 All Services fees are payable annually in advance. Payment for the invoice covering the first year of any Order is due and payable within thirty (30) days of the effective date of the Order. Thereafter, Finalsite will invoice Customer for each subsequent annual period on each annual anniversary of the effective date of the relevant Order. All invoices shall be due and payable within thirty (30) days of invoice date. After thirty (30) days from the invoice date, all overdue unpaid amounts shall carry interest at the rate of 1.5% per month, or the highest rate allowed by applicable law, whichever is less, until payment is received by Finalsite. All fees incurred by Finalsite for collections (including attorneys' fees) must be

paid or reimbursed by the Customer. All invoices shall be sent to Customer at the billing address set forth in the Order.

15.04 If any amount owing by Customer under this Agreement for 60 days or more, Finalsite may, without limiting its other rights and remedies, suspend Services to Customer until such amounts are paid in full. Finalsite will give Customer at least 10 days' prior notice that Customer's account is overdue before suspending Services to Customer.

15.05 Customer shall be responsible for the payment of, or reimbursement of Finalsite for, any applicable present or future services, sales, use, excise, goods, property, value added or other taxes or duties levied against or upon the provision of SaaS Services (excluding taxes based upon Finalsite's net income). Upon request, Customer shall furnish to Finalsite evidence of payment of any taxes payable by Customer. If Customer is exempt from the payment of any such taxes, Customer will provide Finalsite with a valid tax exemption certificate authorized by the appropriate taxing authority.

16. Confidentiality

16.01 In the course of performance of this Agreement, the Parties may receive or have access to information that is confidential to one or the other Party and a Party's Authorized Users (collectively, "Confidential Information"). Confidential Information shall mean non-public materials and information, in whatever form, written, oral or otherwise, that include, but shall not be limited to (i) the SaaS Services, including any modules, functionality or content licensed by Finalsite from third parties; (ii) the distinctive methods or procedures which Finalsite uses in the design, development, licensing, support, or maintenance of the SaaS Services, (iii) the terms and pricing under this Agreement, (iv) each Party's business processes and strategies, (v) all portions of the Customer Materials which are treated as confidential by Customer; (vi) all Personal Information and Student Data; and (v) all information clearly identified by either Party as confidential, provided however that a party's Confidential Information shall not include information that: (a) is or becomes generally available to the public through no act or omission of the other Party; (b) was in the other Party's lawful possession prior to the disclosure and had not been obtained by the other Party either directly or indirectly from the disclosing Party or from a third party whom the

receiving Party knows or should know is under an obligation of confidentiality with the owner of the Confidential Information; (c) is lawfully disclosed to the other Party by a third party without restriction on disclosure; or (d) is independently developed by the other Party.

16.02 Each Party agrees to hold the other Party's Confidential Information in confidence during the Term of this Agreement and following termination for any reason. Except for disclosure to a Party's subcontractors and third party service providers who are bound by confidentiality obligations with respect to such Confidential Information and as otherwise provided in the Agreement, each Party agrees not to make the other Party's Confidential Information available in any form to any third party or to use the other Party's Confidential Information for any purpose not intended under this Agreement. Each Party agrees to take all reasonable steps to ensure that Confidential Information is not disclosed or distributed by any person or entity in violation of the terms of this Agreement. Following receipt of a written request and promptly following termination of this Agreement, the other Party shall return to the requesting Party, in whole or in part, the Confidential Information that has been disclosed in tangible form. Each Party may retain a copy of Confidential Information solely for archival purposes.

17. Representations, Warranties & Disclaimers

17.01 The SaaS Services will substantially perform in all material respects the functions described in Finalsite's then-current standard user guides and administrative guides for the applicable SaaS Services when used and/or accessed in accordance with the terms and conditions of this Agreement and the applicable Order. If SaaS Services fail to so perform, Customer must provide written notice to Finalsite and Customer's sole remedy will be for Finalsite to use commercially reasonable efforts to provide modifications or fixes with respect to the applicable non-conformity. The foregoing are excluded : (i) Customer or its Authorized Users use and/or access the SaaS Services in a manner which is not in conformance with the terms and conditions of this Agreement and any Order; (ii) Customer or its Authorized Users use the SaaS Services with third party data, software or hardware which is incompatible with the SaaS Services; (iii) errors occur in the SaaS Services resulting from Customer's or its representatives' configuration or manipulation of the SaaS

Services, in each case not specifically recommended in writing by Finalsite; or (iv) reduced performance or non-availability of the SaaS Services result from failure of network connections, or other factors, beyond the reasonable control of Finalsite.

17.02 Finalsite represents, warrants and covenants that: (i) this Agreement constitutes the valid and binding agreement of Finalsite, duly authorized by all necessary action on the part of Finalsite; and (ii) the execution, performance and delivery of this Agreement by Finalsite are within Finalsite's corporate powers and do not and will not violate (a) the articles of incorporation or bylaws of Finalsite, (b) any law, rule, regulation, judgment, order or decree applicable to Finalsite's performance of its obligations hereunder or contravene or cause a default under any license, franchise, permit or other similar authorization held by Finalsite, or any agreement to which Finalsite is a party, or (c) require the consent or other action of any person or entity which has not been obtained prior to execution of this Agreement.

17.03 Customer represents, warrants and covenants that: (i) this Agreement constitutes the valid and binding agreement of Customer, duly authorized by all necessary action on the part of Customer; (ii) Customer has full authority to act on its behalf as contemplated by this Agreement; and (iii) the execution, performance and delivery of this Agreement by Customer are within Customer's organizational powers, have been duly authorized by all necessary action on the part of the Customer, and do not and will not violate (a) the applicable organizational documents of Customer, (b) any applicable law, regulatory requirement, judgment, order or decree or cause a default under any license, franchise, permit or other similar authorization held by Customer, or any agreement to which Customer is a party, or (c) require the consent or other action of any person or entity (including in respect of, or filing with, any governmental body, agency or official) which has not been obtained prior to execution of this Agreement.

17.04 It is Customer's responsibility to determine the suitability of the SaaS Services for Customer's use. EXCEPT AS EXPRESSLY STATED IN THIS AGREEMENT, AND TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, FINALSITE AND ITS LICENSORS MAKE NO, AND HEREBY DISCLAIM ANY, REPRESENTATION, WARRANTY OR GUARANTY, WHETHER EXPRESS, IMPLIED, STATUTORY OR

OTHERWISE, WITH RESPECT TO THE SERVICES PROVIDED UNDER THIS AGREEMENT, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTY: (1) OF MERCHANTABILITY; (2) OF FITNESS FOR A PARTICULAR PURPOSE; (3) ARISING FROM COURSE OF PERFORMANCE, COURSE OF DEALING, OR USAGE OF TRADE; OR (4) OF NON-INFRINGEMENT OF THIRD PARTY RIGHTS. EXCEPT AS SET FORTH IN THIS SECTION, THE SERVICES ARE PROVIDED “AS IS”, WITHOUT ANY FURTHER WARRANTIES OF ANY KIND. FINALSITE AND ITS LICENSORS MAKE NO WARRANTY THAT OPERATION OF THE SAAS SERVICES WILL BE UNINTERRUPTED OR ERROR FREE OR THAT ALL DEFECTS WILL BE CORRECTED. FINALSITE AND ITS LICENSORS MAKE NO, AND HEREBY DISCLAIM ANY, REPRESENTATION, WARRANTY OR GUARANTY, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, REGARDING ANY THIRD PARTY TECHNOLOGY.

17.05 EXCEPT TO THE EXTENT EXPRESSLY PROHIBITED BY LAW, FOR ALL CLAIMS BY CUSTOMER, WHETHER SUCH CLAIMS ARE MADE IN CONTRACT, TORT, OR OTHERWISE, CUSTOMER’S POTENTIAL RECOVERY SHALL BE LIMITED TO THE ACTUAL, DIRECT DAMAGES SUFFERED BY CUSTOMER UP TO THE ACTUAL AMOUNT PAID OR PAYABLE BY CUSTOMER TO FINALSITE UNDER THE ORDER UNDER WHICH THE CLAIM AROSE DURING THE TWELVE (12) MONTHS PRIOR TO THE INITIAL ASSERTION OF CLAIM(S) FOR THE SPECIFIC SERVICE(S) GIVING RISE TO SUCH CLAIM(S).

17.06 EXCEPT TO THE EXTENT EXPRESSLY PROHIBITED BY LAW, IN NO EVENT SHALL FINALSITE OR ITS SUPPLIERS, LICENSORS, SERVICE PROVIDERS AND/OR SUBCONTRACTORS BE LIABLE FOR ANY INDIRECT, INCIDENTAL, PUNITIVE, EXEMPLARY, SPECIAL OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, LOSS OF PROFIT OR COSTS OF SUBSTITUTE SERVICES) SUFFERED BY CUSTOMER, HOWEVER CAUSED, REGARDLESS OF THE THEORY OF LIABILITY, WHETHER IN CONTRACT, TORT, PRODUCT LIABILITY OR OTHERWISE, EVEN IF FINALSITE HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY, OR HAS CONSTRUCTIVE KNOWLEDGE, OF SUCH DAMAGES, AND NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE. EXCEPT AS EXPRESSLY SET FORTH IN THIS

AGREEMENT, THIS AGREEMENT SHALL NOT CONVEY UPON ANY THIRD PARTY ANY RIGHTS HEREUNDER, AND NO THIRD PARTY SHALL BE DEEMED A THIRD PARTY BENEFICIARY.

17.07 In the event the Services described in an Order include implementation of procedures or criterial specified by Customer (such as Customer's admission criteria and enrollment procedures), Finalsite expressly disclaims all liability associated with the content such procedures and criteria. Customer is solely responsible for determining the scope and extent of Services provided by Finalsite, and Customer is solely responsible for reviewing the Services provided by Finalsite on Customer's behalf to ensure compliance with Customer's procedures and/or criteria. FINALSITE ASSUMES NO RESPONSIBILITY OR LIABILITY WITH RESPECT TO WHETHER THE CUSTOMER'S PROCEDURES OR CRITERIA COMPLY WITH APPLICABLE LAW OR REGULATORY REQUIREMENTS. HOWEVER, TO THE EXTENT THAT CUSTOMER'S PROCEDURES OR CRITERIA VIOLATE ANY APPLICABLE LAWS OR REGULATORY REQUIREMENTS, FINALSITE RESERVES THE RIGHT TO REFUSE TO IMPLEMENT SUCH PROCEDURES OR CRITERIA WITHOUT LIABILITY TO CUSTOMER.

18. Modifications/ Amendments.

This Agreement (including any Order and/or SOW) can only be modified by a written agreement signed by persons authorized to sign agreements on behalf of each of the Parties.

19. Waiver.

No failure to exercise and no delay in exercising on the part of either Party, or partial exercise, shall operate as a waiver of any right under this Agreement. A waiver on one occasion shall not operate as a waiver on other occasions.

20. Severability.

If any term or provision of this Agreement or application of the terms of this Agreement to the Parties shall to any extent be held invalid or unenforceable by a court of competent

jurisdiction, then such invalidity will not affect the remainder of this Agreement and each other term and provision shall be valid and enforceable to the fullest extent permitted by law.

21. Relationship of Parties.

The Parties are independent contractors and will have no power or authority to assume or create any obligation or responsibility on behalf of each other. This Agreement will not be construed to create or imply any partnership, agency or joint venture, association, or other form of agency relationship between the Parties. A Party and its respective personnel shall not be eligible to participate in any employee welfare or other benefit plans, however characterized, which may be maintained by the other Party. Each Party agrees to assume all responsibility and liability for any and all federal and state employers' liability, workers' compensation, social security and unemployment insurance requirements with respect to its respective personnel. Each Party agrees to pay and report (or require to be paid and reported) all federal, state and local income, employment and payroll withholding taxes and other governmental taxes or charges for its respective personnel as may be applicable.

22. Assignment.

This Agreement may not be transferred or assigned directly or indirectly by Customer, in whole or in part, without the prior written consent of Finalsite, which consent shall not be unreasonably withheld.

23. Force Majeure.

Either Party will be excused from delays in performing or from failing to perform its obligations under this Agreement (except for payment obligations which shall not be so excused) to the extent the delays or failures result from causes beyond the reasonable control of the Party. Without limiting the generality of the foregoing, such causes include acts of God, the public enemy, fires, floods, storms, earthquakes, riots, terrorism, strikes, blackouts, wars or war operations, restraints of government, including public states of emergency, utility or communications failures, computer hackers, denial of service attacks,

software viruses, telecommunications slow-downs or failure, erroneous data transmission, or causes which could not with reasonable diligence be controlled or prevented by the Party. However, to be excused from delay or failure to perform, the Party must promptly provide written notice to the other Party and act diligently to remedy the cause of the delay or failure.

24. Entire Agreement.

This Agreement, including any and all Orders, SOWs, Exhibits, Schedules, Appendices, Attachments and material incorporated by reference, contains the entire agreement of the Parties relating to the rights granted and obligations assumed in this Agreement. This Agreement represents the complete and final agreement of the Parties and supersedes and replaces all prior or contemporaneous oral or written agreements, understandings or commitments between the Parties, including any purchase order. For clarity, while Customer may utilize a purchase order for its internal administrative purposes, any terms or conditions in any such purchase order shall be deemed null and void and the terms and conditions of this Agreement shall solely govern and control.

25. Mutual Indemnification.

25.01 Finalsite shall defend, indemnify and hold Customer and Customer's officers, directors, employees, and agents harmless from and against any and all third party claims, costs, damages, losses, liabilities and expenses (including reasonable attorneys' fees and costs incurred by Finalsite in defending a covered claim) to the extent caused by (i) any willful misconduct of Finalsite ; and/or (ii) the infringement by the SaaS Services, in their as-delivered, unaltered form, of a U.S. or EEA registered copyright, a U.S. or EEA patent issued as of the date on which the applicable Order is entered into by the Parties, or a U.S. or EEA registered trademark of a third party; provided that Customer shall (a) promptly give written notice of such claim to Finalsite; (b) give Finalsite sole control of the defense and settlement of such claim; and (c) promptly provide to Finalsite all available information and assistance reasonably requested by Finalsite in defending such claim. Finalsite shall have no indemnification obligation, and Customer shall defend, indemnify and hold Finalsite and its officers, directors, employees, attorneys and agents harmless from and against any and

all third party claims arising from any alleged infringement of any third party intellectual property rights arising from the combination of any SaaS Services with any of Customer's products, service, content, web service, hardware and/or business process(s).

25.02 Except to the extent expressly prohibited by applicable law, including applicable laws providing for the sovereign immunity of government entities, Customer shall indemnify and hold Finalsite, its licensor's and each such party's affiliates, officers, directors, employees, attorneys and agents harmless from and against any and all third party claims, costs, damages, losses, liabilities and expenses (including attorneys' fees and costs) to the extent caused by : (i) any willful misconduct of Customer; (ii) the infringement by the Customer Materials, and/or any Third Party Technology provided to Finalsite or input into the SaaS Services by Customer or its Authorized Users, of the intellectual property rights of a third party; (iii) the nature, substance or content of the Customer Materials (such as a defamation claim, an invasion of privacy claim, a claim arising from lack of consent to use the Customer Materials, and/or other claims; (iv) Customer's failure to assume liability or responsibility where it expressly agrees to do so hereunder; and (v) Customer's or its Authorized Users' failure to access and use the SaaS Services in compliance with the restrictions or prohibitions set forth in this Agreement and/or applicable law and regulation; provided in any such case that Finalsite (a) gives written notice of the claim promptly to Customer; (b) gives Customer sole control of the defense and settlement of the claim (provided that Customer may not settle or defend any claim unless Customer unconditionally release Finalsite of all liability and such settlement does not affect Finalsite' business or Service); (c) provides to Customer all reasonably available information and assistance; and (d) has not compromised or settled such claim.

26. Venue and Applicable Law.

This Agreement shall be governed, construed, and interpreted in accordance with the laws of the State of Connecticut, USA, excluding conflict of law principles. The original of this Agreement has been written in English and English is the governing language of this Agreement. Customer waives any right it may have under the law of its territory to have this Agreement interpreted by or written in the language of the territory. In any action or

proceeding to enforce rights under this Agreement, the prevailing party will be entitled to recover reasonable costs and attorneys' fees. Any disputes arising out of this Agreement or the breach thereof shall be resolved in the state or Federal courts located in Hartford County, Connecticut USA.

SCHEDULE 1

Service Level Agreement

This SLA sets forth the Service Level(s) applicable to the Hosting Services and Support Services provided by Finalsite for the Finalsite SaaS Services. This SLA forms a part of the Agreement between Customer and Finalsite with respect to the provision of the SaaS Services by Finalsite and is incorporated into the Agreement by reference.

1.Hosting/ Availability of the SaaS Services

Service Level	Service Level Commitment	Measurement Window
Availability	99.5%	Monthly

For Purposes of this SLA, the following definitions shall apply:

"Availability" shall mean the portion (in percentage terms) of Scheduled Uptime that the Hosting Services are actually Available for Use.

"Available For Use" shall mean that all of the supported functions and features of the Hosting Services are capable of sending and receiving data to and from the Internet.

"Scheduled Uptime" shall mean the difference between (i) the total time Available for Use during each month and (ii) the sum of the time during which Finalsite may perform Scheduled Maintenance plus Excluded Time (as defined below).

"Scheduled Maintenance" shall mean maintenance performed by Finalsite during regularly scheduled maintenance windows, which normally shall occur during off-peak hours, or such other times Finalsite may determine, provided it shall provide Customer at least three (3) days' advance notice of such maintenance ("Scheduled Maintenance Window"). Notice of Scheduled Maintenance may be by email to Customer.

"Excluded Time" shall mean any period of time that the Hosting Services are not Available For Use due to the following:

- Emergency maintenance;
- Interruptions in third party networks that prevent Internet users from accessing the Hosting Services; or
- Interruptions in utility service, provided that the Finalsite hosting environment is served by redundant utility connections entering the facility at which the Hosting Services are provided.

2. Availability Service Credits

a. Customer must notify Finalsite in writing of any failure to meet the Availability Service Level and request a Service Level Credit, if appropriate.

b. In the event Finalsite fails to meet the Availability Service Level Commitment more than three (3) times in any rolling twelve (12) month period, upon the written request of Customer, Finalsite will extend five (5) days of hosting service to the Customer at no additional charge (the "Service Credits"). Such Service Credits will be allocated to the Customer annually on the anniversary date of the applicable Order for the SaaS Services.

c. The Service Credits described above shall be the sole and exclusive remedy for Finalsite's failure to meet the Availability Service Level Commitment.

3. Backup Process

Finalsite will back-up or cause daily and weekly back-ups of Data (excluding Customer

logos and trademarks) on-site and to an off-site location chosen by Finalsite.

4.Hosting / Bandwidth / Storage Obligations

Finalsite will provide and will be responsible for creating and maintaining the hosting, bandwidth and storage obligations as set out within the Order. If the Customer exceeds the limits defined in the Order, Finalsite shall not be held liable for any performance related issues which arise from use outside of these limits and may, at its discretion, charge for any excess use of these obligations.

SCHEDULE 2

Additional Privacy Terms

For Customers located in the United States, the following terms shall apply and are incorporated into the Master Terms:

1. Student Data.

1.01 Student Information, Student records and Student-generated content (collectively, "Student Data") is the property of the applicable student or legal guardian of the student and not the property, or under the control, of Finalsite. During the Term of this Agreement, Customer shall retain control of all Student Data maintained in connection with the Services.

1.02 At any time during the Term of this Agreement, Customer may request deletion of any Student Data in Finalsite's possession by providing a written request to Finalsite signed by a duly authorized representative of Customer specifying: (i) the name of the applicable

student(s); (ii) a detailed description of the Student Data to be deleted; (iii) providing contact information of an individual authorized by Customer to answer questions and provide additional information about such request. Such requests must be addressed to the following address: Privacy Officer, Finalsite, 655 Winding Brook Drive, Glastonbury, CT 06033 or privacy@finalsite.com (which address may be amended by Finalsite from time to time upon notice to Customer). Customer shall be solely responsible and liable to the Student and any other party, and shall ensure that Finalsite shall have no responsibility or liability, in connection with the content of such deletion request (including any errors contained therein) or Finalsite's deletion of Student Data in accordance with such request.

1.03 Finalsite shall take reasonable commercial measures designed to ensure the security and confidentiality of all Student Data. Finalsite and its employees, agents and contractors shall use Student Data only for purposes for which it may utilize Customer Materials as described in Section 7.02 above.

1.04 Student Data may include "education records" as defined under the Family Educational Rights and Privacy Act of 1974, 20 USC 1232g and its implementing regulations, as they may be amended from time to time ("FERPA"). To the extent that Finalsite collects or processes personally identifiable information in education records in the course of providing Services under this Agreement, then it does so as an outsourced institutional function pursuant to FERPA 34 CFR Part 99.31(a)(1) and is designated by Customer for these purposes as a "school official" with legitimate educational interests. In this regard, Finalsite will comply with its responsibilities as a school official under FERPA. Similarly, Customer shall comply with the responsibilities applicable to Customer under FERPA.

1.05 Revisions or corrections to Student Data may only be made by Authorized Users of Customer and not the student, parent or legal guardian directly. A student, parent or legal guardian of a student may review personally identifiable information contained in the Student Data directly through use of the SaaS Services and may correct erroneous information, if any, to such information by informing the Customer in writing specifying: (i) the name of the applicable student; (ii) a detailed description of the Student Data to be

corrected; (iii) the appropriate correction, if known. In the event Finalsite receives a correction request directly concerning any Student Data, it will notify Customer promptly and direct the student, parent or legal guardian to the Customer for a response, or upon the written request of Customer containing such information as described in this subsection, Finalsite will correct the applicable Student Data using the information contained in Customer's written notice. Such requests must be addressed to Finalsite at the address set forth in Section 9.02 above. Customer shall be solely responsible and liable to the Student and any other party, and shall ensure that Finalsite shall have no responsibility or liability in connection with the content of such modification request (including any errors contained therein) or Finalsite's revisions or corrections to Student Data which are made in response with such request.

1.06 Finalsite will report in writing to Customer after its discovery of any unauthorized release, disclosure or acquisition of Student Data not permitted or required by this Agreement or any Order in accordance with the requirements of applicable law. Following discovery, Finalsite will conduct an investigation to determine the nature and scope of such unauthorized release, disclosure or acquisition and the identity of the affected students. Finalsite will use reasonable efforts to mitigate the potential harm caused by such unauthorized release, disclosure or acquisition.

1.07 Finalsite will not sell, rent or trade any Student Data, except in connection with the change of control or acquisition of Finalsite's business and in such event the successor-in-interest to Finalsite shall be subject to the provisions of this Agreement.

1.08 Upon termination of this Agreement and all Orders hereunder, Student Data shall be deleted and not retained by Finalsite and Customer shall not have access to any Student Data following the effective date of termination unless a student, parent or legal guardian of a student establishes or maintains an electronic account with Finalsite for the purpose of storing student-generated content.

1.09 For purposes of this Section, the following definitions shall apply:

(a) "Student information" means personally identifiable information or material of a student

in any media or format that is not publicly available and is any of the following: (i) Created or provided by a student or the parent or legal guardian of a student, to Finalsite in the course of the student, parent or legal guardian using the SaaS Services for school purposes, (ii) created or provided by an employee or agent of Customer for school purposes, or (iii) gathered by Finalsite through the operation of the SaaS Services and identifies a student, including, but not limited to, information in the student's records or electronic mail account, first or last name, home address, telephone number, date of birth, electronic mail address, discipline records, test results, grades, evaluations, criminal records, medical records, health records, Social Security number, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious affiliations, text messages, documents, student identifiers, search activity, photographs, voice recordings, survey responses or behavioral assessments;

(b) "Student record" means any information directly related to a student that is maintained by the Customer or any information acquired from a student through the use of the SaaS Services, except "student record" does not include De-identified student information (defined below) allowed under this Agreement to be used by Finalsite for the purposes described in Section 10.03 below.;

(c) "Student-generated content" means any student materials created by a student including, but not limited to, essays, research papers, portfolios, creative writing, music or other audio files or photographs; "student-generated content" does not include student responses to a standardized assessment.

(d) "De-identified student information" means any Student Information that has been altered to prevent the identification of an individual student.

For Customers located outside of the United States, the following terms shall apply and are incorporated into the Master Terms. These terms may co-exist with the terms of Finalsite's standard Data Processing Addendum ("DPA") as applicable to the Customer's country of origin. In the event of a conflict between these terms and the current DPA, the DPA shall control.

1. Additional Definitions.

(a) “Data Controller” shall have the same meaning as set out in the Data Protection Legislation.

(b) “Data Processor” shall have the same meaning as set out in the Data Protection Legislation.

(c) “Data Protection Legislation” means all data protection and privacy laws and regulations anywhere in the world which are applicable to that Party in exercising its rights or fulfilling its obligations under the Agreement, including the GDPR, the laws and regulations of the European Union (“EU”), the European Economic Area (“EEA”) and their member states applicable to the Processing of Personal Data under the Agreement.

(d) “Data Subject” means a natural person to whom Personal Data relates.

(e) “GDPR” means the General Data Protection Regulation ((EU) 2016/679).

(f) “Personal Data” shall have the same meaning as set out in the Data Protection Legislation.

(g) “Process” shall have the same meaning as set out in the Data Protection Legislation.

2. Both Parties will comply with all applicable requirements of the Data Protection Legislation. This clause is in addition to, and does not relieve, remove or replace, a party’s obligations under the Data Protection Legislation.

3. The Parties acknowledge that for the purposes of the Data Protection Legislation, the Customer is the Data Controller and Finalsite is the Data Processor.

4. Customer will ensure that it has all necessary appropriate consents and notices in place to enable lawful transfer of the Personal Data to Finalsite for the duration and

purposes of this Agreement so that Finalsite may lawfully use, process and transfer the Personal Data in accordance with this Agreement on the Customer's behalf.

5. Finalsite shall, in relation to any Personal Data Processed in connection with the performance by Finalsite of its obligations under this Agreement:

(a) Process that Personal Data only on the written instructions of the Customer or the relevant Data Protection Legislation. Finalsite is required by the laws of any member of the European Union or by the laws of the European Union applicable to Finalsite to process Personal Data (Applicable Laws). Where Finalsite is relying on laws of a member of the EU or European Union law as the basis for processing Personal Data, Finalsite shall promptly notify the Customer of this before performing the Processing, unless those Applicable Laws prohibit Finalsite from so notifying the Customer;

(b) ensure that it has in place appropriate technical and organisational measures, reviewed and approved by Finalsite, to protect against unauthorised or unlawful Processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data, appropriate to the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures (those measures may include, where appropriate, pseudonymizing and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of its systems and Services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the technical and organisational measures adopted by it).

(c) not transfer any Personal Data outside of the EEA unless the following conditions are fulfilled:

(i) the Customer or Finalsite has provided appropriate safeguards in relation to the transfer;

(ii) the data subject has enforceable rights and effective legal remedies;

(iii) Finalsite complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred; and

(iv) Finalsite complies with reasonable instructions notified to it in advance by the Customer with respect to the processing of the Personal Data;

(d) notify the Customer immediately if it receives:

(i) a request from a Data Subject to have access to that person's Personal Data;

(ii) a request to rectify, block or erase any Personal Data;

(iii) any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation (including any communication from the Information Commissioner);

(e) assist the Customer, at the Customer's cost, in responding to any request from a Data Subject and in ensuring compliance with its obligations under the Data Protection Legislation with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators;

(f) notify the Customer without undue delay on becoming aware of a Personal Data breach;

(g) at the written direction of the Customer, delete or return Personal Data and copies thereof to the Customer on termination of the Agreement unless required by relevant Data Protection Legislation to store the Personal Data; and

(h) maintain complete and accurate records and information to demonstrate its compliance with this Schedule 2 and allow for audits as required by applicable law by the Customer or the Customer's designated auditor in accordance with the terms of Finalsite's DPA.

3. The terms and conditions of Finalsite's DPA, to the extent applicable to Customer's country of origin, shall apply to this Agreement and are hereby incorporated by reference.

4. Either Party may, at any time on not less than 30 days' advance written notice to Customer, revise the terms of this Schedule 2 by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme.

5. This Agreement does not transfer ownership of, or create any Orders (implied or otherwise), in any Intellectual Property Rights in any (non-personal) data.

6. The provisions of this Schedule 2 shall survive termination of the Agreement for so long as Finalsite has access to Personal Data provided under this Agreement.

Schedule 3

DATA PROCESSING ADDENDUM (DPA)

by and between

ACTIVE INTERNET TECHNOLOGIES LLC DBA FINALSITE

(including its affiliates)655 Winding Brook Drive

Glastonbury, CT 06033 Connecticut USA in this DPA, "**Finalsite**" or "**Processor**"

and

School Name

represented by **Title**: **Name**

Address 1

Address 2
in this DPA, "**Client**" or "**Controller**"

PREAMBLE

- Whereas **Finalsite** (including its affiliates) offers information technology services to **Client** such as provision of software as a service and hosting the Client's website and providing support for the website.

- Whereas **Client** has signed an agreement with **Finalsite** (the "Agreement") or one of its affiliates for the development of Client's website and provision of related services including hosting of Client's website within the European Union("EU") and/or the United Kingdom ("UK").

- Whereas on the purpose of this **Data Processing Addendum ("DPA")** is to supplement the Agreement to provide for the protection of Personal Data in accordance with the requirements of EU and UK law.

- Whereas **Finalsite** and **Client** take into account that the EU-U.S. Privacy Shield Framework is no longer legally recognized in the European Union and to the known situation of the UK as leaving the European Union which may lead to a situation in which the UK may not be deemed to be comparable to the European data privacy legislation.

- Whereas **Finalsite** and **Client** agree on that all and any data of the **Client** have

always to be processed by the **Finalsite** on a legal basis respecting all European data privacy legislations.

• Whereas the UK's data protection system continues to be based on the same rules that were applicable when the UK was a Member State of the EU. The UK has fully incorporated the principles, rights and obligations of the GDPR and the Law Enforcement Directive into its post-Brexit legal system.

• Whereas the effect of this Data Processing Addendum will align with the *sunset clause* of the EU's GDPR adequacy decision for the UK in that any provision within this DPA will also automatically expire four years after their entry into force. It is acknowledged by the **Parties**, that after that period, the adequacy findings might be renewed, however, only if the UK continues to ensure an adequate level of data protection.

i. SCOPE.

This DPA forms part of the underlying agreement, inclusive of any amendments thereto and Orders thereunder under which **Finalsite** provides Services to **Client** ("**Agreement**") and reflects the Parties' agreement about the **Processing** of **Personal Data** (including sensitive data) provided to **Finalsite** in accordance with Data Protections Laws. All capitalized terms not defined in this DPA have the meanings given in the Agreement. This DPA is effective when signed by both Parties.

ii. DEFINITIONS.

In this DPA:

(a) "**Client**" means the relevant entity that has entered into an agreement with **Finalsite** to receive Services.

(b) "**Controller**," "**Data Subject**," "**Security Incident**" and "**Processor**" shall have the meanings given in **GDPR**.

(c) "**Personal Data**" means any information relating to an identified or identifiable natural person Processed by **Finalsite** on behalf of **Client** under the Agreement. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier.

(d) "**Processing**" (and its variants) means any operation or set of operations performed on **Personal Data**, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

(e) "**Data Protection Laws**" means, in respect of a Party, all data protection and privacy laws applicable to that Party in exercising its rights or fulfilling its obligations under the Agreement, including the laws and regulations of the United Kingdom ("UK"), the European Union ("EU"), the European Economic Area ("EEA") and their member states applicable to the **Processing** of **Personal Data** under the Agreement and the General Data Protection Regulation 2016/679 ("**GDPR**").

(f) "**Data Subject**" means the natural person to whom **Personal Data** relates.

(g) "**Standard Contractual Clauses**", or "**SCCs"** means the **Standard Contractual Clauses** for Data **Processors** established in third countries pursuant to European Commission decision (2010/87/EU) of the Data Protection Directive, as set out in Exhibit A to this DPA, as such SCCs may be updated and from time to time to conform with EU and UK directives.

(h) "**Sub-processor**" means any data processor, including an Affiliate of **Finalsite**, engaged by the **Finalsite** for processing or having authorized access to **Personal Data**.

iii. DATA PROCESSING

(a) The Parties acknowledge and agree that with regard to **Processing Personal Data**, **Client** acts as **Controller** and **Finalsite** acts as **Processor**.

(b) **Finalsite** shall only Process the **Personal Data** in accordance with **Client**'s instructions or as required to comply with any applicable law. This DPA and the Agreement – as far as it contains instructions of the **Client** - are **Client**'s complete and final instructions to **Finalsite** for the **Processing** of **Personal Data**. Any additional or alternative instructions must be agreed upon in writing by the Parties.

(c) **Processing** is carried out in an automated process using the **Finalsite**'s and its Sub-processor's information technology systems and procedures. The **Processing** Operations are further set out in Appendix 1 to the DPA and in the Agreement and relevant Orders.

(d)Each Party shall comply with all laws, regulations and rules applicable to it in the performance of this DPA, including **Data Protection Laws**.

(e) **Finalsite** shall inform **Client** if, in **Finalsite**'s reasonable opinion, an instruction from **Client** conflicts with **Data Protection Laws**. After **Finalsite** so informs **Client**, **Finalsite** shall have no liability for any claim arising from or related to **Processing** of **Personal Data** under this DPA by **Finalsite** in accordance with **Client**'s instructions.

(f) **Client** and **Finalsite** agree that **Personal Data** must be processed only within the EEA or the UK. Any transfer of **Personal Data** outside the EEA or UK is only allowed with prior written consent of **Client** (such consent not to be unreasonably withheld). In this case the following applies: The **Standard Contractual Clauses** apply only to **Personal Data** that is transferred from the EEA or, either directly or via onward transfer, to any country or recipient: (i) not recognized by the European Commission or the UK Information Commissioner's Office as providing an adequate level of protection for personal data, and (ii) not covered by a suitable framework or derogation recognized by the relevant authorities or courts as providing an adequate level of protection for **Personal Data**, including but not limited to Binding Corporate Rules for **Processor**s or consent by the **Data Subject**.

Notwithstanding the foregoing, the **Standard Contractual Clauses** will not apply if **Finalsite** adopts an alternative recognized compliance standard for the lawful transfer of **Personal Data** outside the EEA or UK. In the event of any conflict or inconsistency between this DPA and the **Standard Contractual Clauses** in Exhibit A, as may be amended from time to time, the **Standard Contractual Clauses** shall prevail. In the event the EEA and/or the UK regulatory authorities issue final updated SCCs, the Parties will replace the applicable version of such updated SCCs with those set forth in Exhibit A and shall the applicable version of such SCCs on or prior to the effective date thereof, but in any event without undue delay.

(g) **Finalsite** shall limit access to **Personal Data** to those personnel who require such access to perform the Agreement. **Finalsite** shall ensure that all personnel authorized by **Finalsite** to Process **Personal Data** receive appropriate training on their responsibilities and are subject to contractual obligations of confidentiality that shall survive the termination of their employment and/or contractual relationship.

(h) Upon expiration or any earlier termination of the Agreement, **Finalsite** shall, as set forth in the Agreement, delete or return to **Client** all **Personal Data** in **Finalsite**'s possession; provided, however, that **Finalsite** may retain **Personal Data** as permitted or required to meet its compliance obligations under applicable law.

(i) Upon expiration or any earlier termination of the Agreement, **Finalsite** and the **Client** (acting reasonably and in good faith) will follow the following timeline for the safe and timely deletion of the **Client's Personal Data**:

30 days from expiry/early termination **Finalsite** to provide release / download of Personal Data as reasonably requested by the **Client**

90 days from expiry/early termination **Finalsite** to complete deletion of Personal Data of last and available data back-ups made of the **Client's Personal Data**.

(j) **Finalsite** shall:

(i) to the extent legally permitted, promptly notify **Client** if it receives a request from a **Data**

Subject for access to, correction, amendment or deletion of that personal's **Personal Data**;

(ii) provide reasonable cooperation and assistance to **Client** in relation to handling of a **Data Subject**'s request for access to that person's **Personal Data** to the extent legally permitted and to the extent that **Client** does not have access to such **Personal Data** through its use of the Services.

(iii) If legally permitted, **Client** shall be responsible for any costs arising from **Finalsite**'s provision of such assistance. The latter does not apply in cases where the **Data Subject** contacts the **Finalsite** to receive information and access to personal data with regard to the processing by the **Finalsite** based on the **GDPR**. In this case all and any costs to fulfill the **Data Subject**'s rights are to be borne by the **Finalsite**

(k) **Client** hereby warrants and represents, on a continuous basis throughout the Term, that all **Personal Data** provided or made available by **Client** to **Finalsite** for **Processing** in connection with the Agreement has been collected by **Client** and transmitted to **Finalsite** in accordance with **Data Protection Laws** and **Client** has obtained all necessary approvals, consents, authorizations and licenses from each and every **Data Subject** that may be required under **Data Protection Laws** to enable **Finalsite** to Process the **Personal Data** pursuant to the Agreement and this DPA and to exercise its rights and fulfil its obligations under the Agreement and this DPA.

iv. SUBPROCESSING.

(a) **Client** acknowledges and approves **Finalsite**'s use of its **Sub-processor**s existing as of the Effective Date, (including the **Sub-processor**s set forth in the list attached to this Agreement as Schedule 1) and hereby provides its general authorization to **Finalsite** to appoint **Sub-processor**s to Process **Personal Data** on **Finalsite**'s behalf. A current list of **Sub-processor**s used by **Finalsite** to Process **Personal Data** shall be provided to **Client** upon request.

(b) **Finalsite** shall:

(i) ensure that **Sub-processor**s are contractually obligated to protect **Personal Data** in compliance with **Data Protection Laws** and consistent with the obligations imposed on **Finalsite** in this DPA;

(ii) remain responsible for the acts and omissions of any such **Sub-processor** as if they were the acts and/or omissions of **Finalsite**;

(iii) transfer **Personal Data** outside the EU/EEA/UK if required by the **Client** to perform the Services in compliance with **Data Protection Laws**;

(iv) provide notice to the **Client** of any new or replacement Sub- processors (such as e-mail or in writing) and give the **Client** the opportunity to object to this **Sub-processor** from **Processing** its **Personal Data**. If **Client** does not object in writing within thirty (30) calendar days after receipt of notice of a new **Sub-processor**, the appointment of such Subprocessor shall be deemed approved.

(c) **Finalsite** shall provide to **Client** a copy of any notice it receives from any competent data protection regulator or any **Data Subject** relating to the **Processing** of **Personal Data** and provide **Client** with reasonable assistance and co-operation in responding to such notice.

v. SECURITY.

(a) **Finalsite** shall implement appropriate technical and organizational measures in relation to the **Processing** of **Personal Data** intended to ensure a level of security appropriate to the **Personal Data Processing**, in particular protect against accidental or unlawful destruction, loss or alteration of, unauthorized disclosure of, or access to **Personal Data** transmitted, stored or otherwise Processed by **Finalsite** ("**Security Incident**").

(b) Without undue delay after becoming aware of a **Security Incident**, **Finalsite** shall notify **Client** of the **Security Incident**, provide such information as **Client** may reasonably require

to meet its obligations under applicable law and take steps to remediate the **Security Incident**.

(c) During the term of the Agreement, the **Finalsite** will maintain its self-certification and compliance with Swiss-U.S. and EU-U.S Privacy Shield Framework and Principles issued by the U.S. Department of Commerce (even if not legally enforceable in the EU or UK), both available at https://www.privacyshield.gov/EU-US-Framework (the "Privacy Shield Principles").

vi. AUDIT RIGHTS

(a) If **Client** wishes to audit the **Finalsite**'s premises/server locations or is subject to an audit or investigation from a competent data protection regulator, if required by applicable **Data Protection Laws**, **Finalsite** shall respond to any information requests, and/or agree to submit its premises (in accordance with the access requirements of the hosting agent) and operations to audits, including inspections by **Client** and/or the competent data protection regulator, in each case solely for the purpose of evidencing its compliance with this DPA, provided that:

(i) **Client** shall ensure that all information obtained or generated in connection with any information request, audit or inspection is kept strictly confidential (unless disclosure to a competent data protection regulator or as otherwise required by applicable law);

(ii) **Client** shall ensure that any information request, audit or inspection is undertaken within normal business hours (unless such other time is mandated by a competent data protection regulator) with minimal disruption to **Finalsite**'s and/or its sub-processors' businesses, and acknowledging that such information request, audit or inspection: (a) shall not oblige **Finalsite** to provide or permit access to information concerning **Finalsite**'s internal pricing information or relating to other recipients of services from **Finalsite**; and (b) shall be subject to any reasonable policies, procedures or instructions of **Finalsite**, or its **Sub-processor**s, for the purposes of preserving security and confidentiality (including any requirements

imposed on **Finalsite** or its Sub- processor by its other customers, or business partners);

(iii) **Client** shall give **Finalsite** at least 30 days' prior written notice of an information request and/or audit or inspection (unless the competent data protection regulator provides **Client** with less than 30 days' notice, in which case **Client** shall provide **Finalsite** with as much notice as possible);

(iv) If any information request, audit or inspection relates to systems provided by or on the premises of **Finalsite**'s **Sub-processor**s, the scope of such information request, audit and/or inspection shall be as permitted under the relevant agreement in place between **Finalsite** and the **Sub-processor**.

(v) A maximum of one information request, audit and/or inspection may be requested by **Client** in any twelve (12) month period unless an additional information request, audit and/or inspection is mandated by a competent data protection regulator in writing and each such audit and/or inspection may not exceed two (2) business days in length.

(vi) **Client** shall not be liable for any costs (i) incurred from the **Finalsite** for any assistance, contribution, co-operation, provision of information, or facilitation of any audit or inspection, or other work undertaken pursuant to **Finalsite**'s obligations under this DPA or the audit was required by a competent data protection regulator, the annual audit requested by the **Client** (if elected) in (v) above or otherwise required by applicable law or

(vii) incurred due to **Finalsite**'s breach of its obligations under this DPA or applicable law. The **Client** shall be liable for the reasonable costs incurred by the **Finalsite** due to the **Client**'s breach of its obligations under this Addendum or applicable law

(b) **Finalsite** shall provide **Client** with reasonable assistance with data protection impact assessments or prior consultations with data protection authorities that **Client** is required to carry out under applicable **Data Protection Laws**.

vii. MISCELLANEOUS.

Except as amended by this DPA, the Agreement shall remain in full force and effect and is ratified by the Parties. Any claims arising under this DPA shall be subject to the exclusions, limitations (including any aggregate limitation of liability) and other terms of the Agreement. If the Agreement and this DPA conflict, then this DPA shall control but solely to the extent of the inconsistency. Clause 9 of the **Standard Contractual Clauses** shall apply to this DPA.

CUSTOMER	**FINALSITE**
By:	By:
Name:	Name:
Title:	Title:
Date:	Date:

EXHIBIT A

STANDARD CONTRACTUAL CLAUSES

Controller to Processor

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject

rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties,

accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in

line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records

concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least [Specify time period] in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a

processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to

supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer

pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of the data exporter's State.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the data exporter's State.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Name: _____

Address: _____

Contact person's name: _____

Position: _____

Email: _____ Phone. _____

Activities relevant to the data transferred under these Clauses:

_____

_____

Signature:

Date: _____

Role: ***Controller***

Data importer(s):

Name: **Active Internet Technologies**, LLC dba Finalsite (and its affiliates)

Address: 655 Winding Brook Drive, Glastonbury CT 06029

Contact person's name: _____

Position: _____

Email: _____ Phone. _____

Activities relevant to the data transferred under these Clauses:

_____

_____

Signature:

Date: _____

Role: ***Processor***

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

The personal data transferred concern the following categories of data subjects:

The data exporter may submit **Personal Data** to **Finalsite**, the extent of which is

determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to **Personal Data** relating to the following categories of data subjects:

- Prospective customers, customers, suppliers, authorized agents, minors, subscribers, and vendors of the data exporter (who are natural persons);

- Employees or contact persons of the data exporter's prospective customers, customers, subcontractors, business partners, and vendors (who are natural persons);

- Natural persons authorized by the data exporter to use the services provided by **Finalsite** to the data exporter.

Processing operations

The personal data transferred will be subject to the following basic processing activities:

- The objective of the processing of Personal Data by Finalsite is to provide the Service, pursuant to the Agreement.

Processing Activity Specification

Finalsite and **Client** shall comply with this Schedule.

Any such further written instructions shall be deemed to be automatically incorporated into this Schedule.

Description	Details
Subject matter of the **Processing**	**Finalsite** has built and manages the **Client**'s website and deploys software utilized thereby. As such, it has access to all data contained on these sites/platforms.
Duration of the **Processing**	For the duration of the Agreement between the **Finalsite** and the **Client**.

Nature and purposes of the **Processing**	As the developers and host managers of the platform, **Finalsite** processes/has access to all Personal Data that is contained on the platform. This includes Personal Data that is submitted by the Data Subject as well as Personal Data submitted on behalf of the Data Subject. Any Personal Data that is submitted onto the platform is therefore processed by the **Finalsite**. The website is hosted by or on behalf of **Finalsite** – servers are located in the UK. If the **Client** consents in writing for data to be stored in the US by **Finalsite**, this transfer will be addressed by the **Standard Contractual Clauses**. **Finalsite** can also access website user information – including login information and usage.
Type of **Personal Data**	All data that is submitted by users onto the platform via the webforms or members area or any data capture forms is processed by **Finalsite**. This includes – but is not limited to - school staff names, full contact details, Supporting member names/contact details/addresses. This also includes site usage data, to the extent personally-identifiable.
Categories of **Data Subject**	As above.
Plan for return and destruction of the data once the **Processing** is complete	For the length of time that the website is operational, **Finalsite** will be processing this data. If the website is to be closed, and/or the Agreement between the **Finalsite**/the **Client** is terminated, the data held on the platform will be extracted and returned to the **Client** as the Data **Controller** in an accessible format. Any data on the platform will then be deleted

Categories of personal data transferred

The personal data transferred concern the following categories of data:

The data exporter may submit **Personal Data** to **Finalsite**, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to, the following categories of **Personal Data**:

- Names, titles, position, employer, contact information (email, phone, fax, physical address etc.), identification data, professional life data, personal life data, connection data, or localization data (including IP addresses).

C. COMPETENT SUPERVISORY AUTHORITY

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Processor will implement and maintain the security measures set out in this Appendix 2

("Security Measures"). **Processor** may update or modify such Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services.

1.0 Third Party policies and procedures:

Processor will maintain policies and procedures as set by Google our hosting agent. A link to these policies is found here: https://cloud.google.com/security/compliance/

2.0 Finalsite's policies and procedures:

2.1 Introduction

This Technical and Organizational Data Security Measures articulates the technical and organizational security measures implemented by the **Finalsite** in support of its Security Program.

2.2 The Technical and Organizational Data Security Measures

Finalsite has implemented and maintains a security program that leverages the ISO/IEC 27000-series of control standards as its baseline.

2.3 Access Control of Processing Areas (Physical)

Web applications, communications infrastructure, and database servers of **Finalsite** are located in secure data centers. **Finalsite** has implemented suitable measures in order to prevent unauthorized persons from gaining access to the data processing equipment (namely telephones, database and application servers and related hardware) where **Personal Data** are processed or used.

This is accomplished by:

- Establishing security areas;
- Protection and restriction of access paths;

- Securing the data processing equipment and personal computers;

- Establishing access authorizations for employees and third parties, including the respective documentation;

- Regulations/restrictions on card-keys;

- Restricting physical access to the servers by using electronically-locked doors and separate cages within co-location facilities;

- Access to the data center where **Personal Data** are hosted is logged, monitored, and tracked via electronic and CCTV video surveillance by security personnel; and

- Data centers, where **Personal Data** may be hosted, are protected by security alarm systems, and other appropriate security measures, such as user-related authentication procedures, including biometric authentication procedures (e. g., hand geometry), and/or electronic proximity identity cards with users' photographs.

2.4 Access Control to Data Processing Systems (Logical)

Finalsite has implemented suitable measures to prevent its data processing systems from being used by unauthorized persons.

This is accomplished by:

- Establishing the identification of the terminal and/or the terminal user to the **Finalsite** systems;

- Automatic time-out of user terminal if left idle, identification and password required to reopen;

- Automatic lock out of the user ID when several erroneous passwords are entered.

- Events are logged and logs are reviewed on a regular basis;

- Utilizing firewall, router and VPN-based access controls to protect the private service

networks and back-end-servers;

- Continuously monitoring infrastructure security;
- Regularly examining security risks by internal employees and third party auditors;
- Issuing and safeguarding of identification codes; and
- Role-based access control implemented in a manner consistent with principle of least privilege.
- Access to host servers, applications, databases, routers, switches, etc., is logged.
- Access and account management requests must be submitted through internal approval systems.
- Access must be approved by an appropriate approving authority.
- Passwords must adhere to the **Finalsite** password policy, which includes minimum length requirements, enforcing complexity and set periodic resets.
- Password resets are handled via **Finalsite** ticketing system. New or reset passwords are sent to the employee using internal secure, encrypted email system or by leaving a voicemail for the employee.

Finalsite employs intrusion detection systems and also uses commercial and custom tools to collect and examine its application and system logs for anomalies.

2.5 Access Control to Use Specific Areas of Data Processing Systems

Persons entitled to use the data processing system are only able to access **Personal Data** within the scope and to the extent covered by their respective access permission (authorization) and that **Personal Data** cannot be read, copied, modified or removed without authorization.

This is accomplished by:

- Employee policies and training in respect of each employee's access rights to the **Personal Data**;

- Users have unique log in credentials -- role based access control systems are used to restrict access to particular functions;

- Monitoring activities that add, delete or modify the **Personal Data**;

- Effective and measured disciplinary action against individuals who access **Personal Data** without authorization;

- Release of **Personal Data** to only authorized persons;

- Controlling access to account data and customer **Personal Data** via role-based access controls (RBAC) in compliance with the security principle of "least-privilege";

- Internal segmentation and logical isolation of **Finalsite**'s employees to enforce least-privilege access policies;

- Requirements-driven definition of the authorization scheme and access rights as well as their monitoring and logging;

- Regular review of accounts and privileges (typically every 3-6 months depending on the particular system and sensitivity of data it provides access to);

- Control of files, controlled and documented destruction of data; and policies controlling the retention of back-up copies.

2.6 Availability Control

Finalsite has implemented suitable measures to ensure that **Personal Data** is protected from accidental destruction or loss.

This is accomplished by:

- Global and redundant service infrastructure that is set up with full disaster recovery sites;
- Constantly evaluating data centers and Internet service providers (ISPs) to optimize performance for its customers in regards to bandwidth, latency and disaster recovery isolation;
- Situating data centers in secure co-location facilities that are ISP carrier neutral and provide physical security, redundant power, and infrastructure redundancy;
- Service level agreements from ISPs to ensure a high level of uptime;
- Systems and processes in place to detect and defend against DDoS attacks.

2.7 Transmission Control

Finalsite has implemented suitable measures to prevent **Personal Data** from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media.

This is accomplished by:

- Use of adequate firewall and encryption technologies to protect the gateways and pipelines through which the data travels;
- Sensitive **Personal Data** is encrypted during transmission using up to date versions of TLS or other security protocols using strong encryption algorithms and keys;
- Certain types of customer Sensitive **Personal Data** and other confidential customer data are encrypted at rest within the system;
- Protecting web-based access to account management interfaces by employees through encrypted TLS

- End-to-end encryption of screen sharing for remote access, support, or real time communication;

- Use of integrity checks to monitor the completeness and correctness of the transfer of data.

2.8 Input Control

Finalsite has implemented suitable measures to ensure that it is possible to check and establish whether and by whom **Personal Data** have been input into data processing systems or removed.

This is accomplished by:

- Authentication of the authorized personnel;

- Protective measures for **Personal Data** input into memory, as well as for the reading, alteration and deletion of stored **Personal Data**, including by documenting or logging material changes to account data or account settings;

- Segregation and protection of all stored **Personal Data** via database schemas, logical access controls, and/or encryption;

- Utilization of user identification credentials;

- Physical security of data processing facilities;

- Session timeouts.

2.9 Separation of Processing for Different Purposes

Finalsite has implemented suitable measures to ensure that **Personal Data** collected for different purposes can be processed separately.

2.10 Documentation

Finalsite keeps documentation of technical and organizational measures in case of audits and for the conservation of evidence. **Finalsite** takes reasonable steps to ensure that persons employed by it and other persons at the place of work, are aware of and comply with the technical and organizational measures set forth in this document.

2.11 Monitoring

Finalsite does not access **Client Personal Data**, except to provide services to the **Client** which **Finalsite** is obligated to perform, to monitor, analyze and improve the services, in support of the **Client** experience, as required by law, or on request by **Client**; **Finalsite** has implemented suitable measures to monitor access restrictions of **Finalsite**'s system administrators and to ensure that they act in accordance with instructions received.

This is accomplished by:

- Individual appointment of system administrators;

- Adoption of suitable measures to register system administrators' access logs to the infrastructure and keep them secure, accurate and unmodified for a reasonable period of time;

- Keeping an updated list with system administrators' identification details (e.g. name, surname, function or organizational area) and responsibilities.

Definitions

"Personal Data" means any information directly or indirectly relating to any identified or identifiable natural person.

"Sensitive Personal Data" means **Personal Data** (1) consisting of an individual's first name and last name, or first initial and last name, in combination with some other data element that could lead to identify theft or financial fraud, such as a government issued identification number, financial account number, payment card number, date of birth, mother's maiden name, biometric data, electronic signature, health information, or (2)

consisting of log-in credentials, such as a username and password or answer to security question, that would permit access to an online account or an information system; or (3) revealing the personal health information (PHI) of a natural person.

"Security Framework" refers to the collection of **Finalsite**'s policies and procedures governing information security, including, but not limited to, policies, trainings, education, monitoring, investigation and enforcement of its data management and security efforts.

ANNEX III

LIST OF SUB-PROCESSORS

The controller has authorized the use of the following sub-processors:

Sub-Processor	Web Address	Sub-Processor Details and Location	Purpose of Sub-Processor
Algolia	algolia.com	www.algolia.com/policies/infrastructure-and-sub-processors/	Hosted search engine for CMS (Content Management System)
authorize.net	authorize.net	www.authorize.net/en-us/about-us/dpa.html	Payment processing (deprecated) for EMS (Enrollment Management System)
			Cloud hosting,

AWS	aws.amazon.com	aws.amazon.com/compliance/gdpr-center	data storage for EMS
Beefree	beefree.io	beefree.io/sub-processors	Email builder and designer for CMS
Box	box.com	box.com/gdpr	Cloud Content Management (deprecated) LMS
Cloudflare	cloudflare.com	www.cloudflare.com/gdpr/subprocessors	Web-infrastructure and website-security services for CMS
Cloudinary	cloudinary.com	cloudinary.com/trust/subprocessors	Cloud-based image and video management services for CMS
Datadog	datadoghq.com	datadoghq.com/legal/privacy	Application performance monitoring suites for CMS
Elastic	elastic.co	www.elastic.co/gdpr	Log hosting
Google	cloud.google.com	cloud.google.com/terms/subprocessors	Cloud-based hosting services for CMS
			Customer

Intercom	intercom.com	www.intercom.com/help/en/articles/1385437-how-intercom-complies-with-gdpr	Support, documentation for SchoolAdmin for EMS
Mailgun	mailgun.com	www.mailgun.com/gdpr	Cloud-based email service for sending, receiving and tracking email for CMS
Mailup	mailup.com	www.mailup.com/gdpr-infrastructure	Email marketing platform for sending, automating, tracking emails, newsletters and SMS for CMS
MongoDB	mongodb.com	www.mongodb.com/cloud/trust/compliance/gdpr	Distributed document database for CMS and EMS
NMI	nmi.com	www.nmi.com/gdpr	Payment processing (deprecated) for EMS
		www.pendo.io/pendo-blog/pendo-committed-	Analytics tool

Pendo	pendo.io	compliance-gdpr-regulations/	for CMS and EMS
Postmark	postmarkapp.com	postmarkapp.com/support/article/1168-postmarks-gdpr-compliance	Email sending for EMS
Rollbar	rollbar.com	rollbar.com/compliance/gdpr/#	Error data hosting for EMS
Stripe	stripe.com	stripe.com/guides/general-data-protection-regulation	Payment processing for EMS
Twilio	twilio.com	www.twilio.com/gdpr	App push notifications, SMS and voice notifications for CMS and EMS
Zendesk	zendesk.com	support.zendesk.com/hc/en-us/articles/360022185294	Online Web Support, Knowledge Base, Voice & SMS Software for CMS

GET IN TOUCH

MARKETS

PRODUCTS

COMPANY

POPULAR LINKS