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

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

Name of Contractor	Anthology Inc.
PII Declaration	**Does your organization/software collect student personally identifiable information (PII) or staff PII?** Examples of student PII: a. The student's name; b. The name of the student's parent or other family members; c. The address of the student or student's family; d. A personal identifier, such as the student's social security number, student number, or biometric record; e. Other indirect identifiers, such as the student's date of birth, place of birth, and Mother's Maiden Name; Examples of staff APPR PII: a. Teacher Id, Social Security Number, Employee Number, Biometric Record b. Name, Mother's Maiden Name, Parent's Name c. Birthdate, Place of Birth, Address d. Gender, Race, Salary ☐ IF YOUR ORGANIZATION/SOFTWARE DOES NOT COLLECT PII, CHECK THIS BOX AND SKIP TO THE BOTTOM, SIGN AND SUBMIT.
Description of the purpose(s) for which Contractor will receive/access PII	The nature of the service requires Anthology to process PII for its delivery. Anthology only uses customer data for the delivery of the services and as explicitly permitted in the contracts with our clients. Please see our Privacy Statement: https://www.anthology.com/trust-center/privacy-statement
Type of PII that Contractor will receive/access	Check all that apply: ☑ Student PII ☑ APPR PII

Contract Term	Contract Start Date 07/01/2024 Contract End Date 06/30/2025
Subcontractor Written Agreement Requirement	Contractor will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Contract. (check applicable option) ○ Contractor will not utilize subcontractors. ◉ Contractor will utilize subcontractors.
Data Transition and Secure Destruction	~~Upon expiration or termination of the Contract, Contractor shall:~~ • ~~Securely transfer data to EA, or a successor contractor at the EA's option and written discretion, in a format agreed to by the parties.~~ • ~~Securely delete and destroy data.~~ Please see Section 13 of Anthology's DPA for our Company Policy
Challenges to Data Accuracy	~~Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If a correction to data is deemed necessary, the EA will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA's written request.~~ All of these requests would be done directly with the Customer given their role as Controllers of the information. Anthology cannot be responsible for the accuracy of the information under our Processor role.
Secure Storage and Data Security	Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply) ☑ Using a cloud or infrastructure owned and hosted by a third party. ☐ Using Contractor owned and hosted solution ☐ Other: Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data: Anthology ensures that only authorized personnel have access to information systems and client data, and that client data is only accessed and used in a manner consistent with Anthology's privacy and security policies.
Encryption	Data will be encrypted while in motion and at rest.

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

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

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	We have a dedicated Global Data Privacy Program that uses the high EU GDPR standards as a global baseline to ensure we can meet our obligations & can assist our clients with their obligations under applicable data privacy laws. Good data privacy practices require a solid governance model. At Anthology, data privacy and security are a top priority, & our data privacy governance model ensures that senior mgmt. oversees and supports our data privacy & security efforts through the Compliance Comm.& the Security and Privacy Risk Council, a subcommittee of the Compliance Committee. A network of Data Privacy champions supports our Global Privacy Officer & the privacy team. Staff are made aware of the importance of data privacy and their responsibilities under our internal data privacy policy.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	Anthology has technical and organizational measures to protect Customer's data, including personal information. These measures meet at minimum the level required by applicable laws. Anthology has implemented management controls, admission controls, entry and access controls, transmission, input, and order controls, as well as availability controls. Please refer to Annex B of our DPA for a detailed list of the security measures Anthology has in place for its products, including Blackboard (fka Learn).
3	Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.	All employees and contractors are required to review and acknowledge the information security policies at the start of employment. These policies clearly define expectations, obligations, and responsibilities of employees and contractors. Anthology provides security and privacy awareness training at the start of employment and refresher training on an annual basis.
4	Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.	All employees and contractors are subject to confidentiality agreements and are required to review and acknowledge the information security policies at the start of the employment. As mentioned above, all employees must annually complete the security and privacy awareness training.
5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the EA.	Anthology agrees to uphold our responsibilities under laws governing Personal Information and privacy including breach notification requirements. Anthology has a documented and tested security incident response plan to ensure we can meet our obligations under applicable breach notification laws and our contractual notification obligations. In the event of security incident, this helps ensure that we can notify clients in accordance with our contractual and statutory requirements. Anthology maintains a formal Security Incident Response (SIR) Plan to ensure that it meets its regulatory and contractual obligations to its Clients, partners and to support its internal business objectives. The SIR Plan includes a definition of roles and responsibilities, and procedures for the Incident Response Team (IRT) in handling the incident and following it through to resolution. Procedures include identifying the incident, assigning severity, responding to the incident, containment and mitigation activities, restoring service, communicating findings as needed, and performing after action review. The incident response process is tested regularly via table-top exercises, internal and external audit processes, and is regularly updated incorporating the results of these tests. Security incidents will be notified subject to the terms of the Data Processing Addendum.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Data is deleted (or upon request, returned) at the completion of the contract in accordance with the contractual commitments. Clients can export or archive their courses at any time on demand via Learn SaaS's GUI-based export and archive capability, or clients may request a bulk export of course based backups up to four times per year via submission of a support case.
7	Describe your secure destruction practices and how certification will be provided to the EA.	Upon request, data is deleted from the system following standard practices and the techniques detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual ") and/or NIST 800-88 ("Guidelines for Media Sanitization") to destroy all customer data. A certificate will be provided upon request.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	Providing services to thousands of clients, we cannot accommodate individual clients' policies. Security commitments are addressed in Anthology's Master Services Agreement and the Data Processing Addendum. Anthology has a longstanding and strong commitment to providing secure products and services to clients. In our continuing efforts to improve the security of its solutions, Anthology deploys security controls aligned with industry best practices, such as the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27001, Open Web Application Security Project (OWASP), and National Institute of Standards and Technology (NIST) 800 frameworks. These controls are distilled and incorporated into an
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1	Anthology has a robust product security program that is aligned to NIST standards and is certified to the ISO 27001 standard for information security management systems. As a cloud service provider entrusted with the security of our clients ' data, we have incorporated the ISO 27017 and ISO 27018 controls into our compliance framework. https://www.anthology.com/trust-center/security

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

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

1. A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketing purpose. PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.

2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency. This right may not apply to Parents of an Eligible Student.

3. State and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student's identifiable information.

4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.

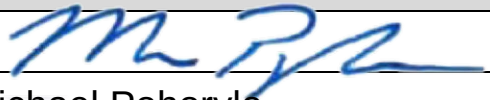
5. A complete list of all student data elements collected by NYSED is available at www.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.

6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to: dpo@wsboces.org. (ii) Complaints may also be submitted to the NYS Education Department at www.nysed.gov/data-privacy-security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to privacy@nysed.gov; or by telephone at 518-474-0937.

7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.

8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.

9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

CONTRACTOR	
[Signature]	
[Printed Name]	Michael Pohorylo
[Title]	Chief Legal Officer
Date:	10/25/2024

Anthology Data Processing Addendum

The terms of this Data Processing Addendum ("**DPA**") are incorporated by reference into the Master Agreement between you and the Anthology group entity listed in the Master Agreement and/or relevant order form, "Anthology", "**we**", "**us**" and "**our**") (the "**Agreement**").

The following provisions shall apply whenever Personal Information is Processed under the Agreement:

1. Definitions

Capitalized terms not defined in this Section have the meaning given in the Agreement.

Applicable Data Privacy Laws means laws and regulations that apply to our and your Processing of Personal Information under this Agreement. In the United States, this may include the Family Education Rights Act ("FERPA"), the Protection of Pupil Rights Amendment ("PPRA"), and the Children's Online Privacy Protection Act ("COPPA"), as well as applicable State student and consumer privacy laws. In the European Union (and outside the EU, if extraterritorially applicable), this will include the General Data Protection Regulation ("GDPR") and the national laws implementing the GDPR, as applicable, In the UK, this will include the UK General Data Protection Regulation ("UK GDPR"). In Australia, this may include the Privacy Act 1998 and amendments. In South Africa, this will include the Protection of Personal Information Act of 2013 ("POPIA").

C2P SCCs means module 2 of the SCCs.

De-Identified Data means information that has all identifying Personal Information obscured or removed such that the remaining information does not reasonably identify an individual nor allow a reasonable person to identify an individual with reasonable certainty.

Individual Right Request means a request from your Authorized Users or other individuals concerning the exercise of their rights available under Applicable Data Privacy Laws in relation to Personal Information, such as the right of access, right to correct, right to restrict Processing, right to erasure ("right to be forgotten"), right to opt-out of the sale of personal information, right to data portability, right to object to the Processing and right not to be subject to an automated individual decision making.

P2P SCCs means module 3 of the SCCs.

Personal Information means information Processed by Anthology on your behalf in connection with the provision of Products and Services pursuant to the Agreement that relates to, describes or is linked to an identified or identifiable individual or, where it is included in the definition of "personal information" or "personal data" under Applicable Data Privacy Laws, a juristic person. For clarity and without limitation, Personal Information may include: (i) in the United States, personal information contained in educational records, as defined by the Family Educational Rights and Privacy Act ("FERPA"), 20 U.S.C. § 1232(g), and/or "student data" or "covered information" as such terms are defined by applicable State student data privacy laws; and (ii) in other jurisdictions, "personal information" or "personal data" as such terms are defined by the Applicable Data Privacy Laws in those jurisdictions.

Processing or **Process** means any operation or set of operations which is performed on Personal Information such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction. For the avoidance of doubt Processing shall include all means, operations and activities performed on Personal Information that are defined as processing under GDPR.

Security Incident means a breach of security that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Information.

Service Providers (Sub-processors) means Anthology affiliates and subsidiaries or third-party vendors which we engage in connection with the Agreement and which Process Personal Information on behalf of us and under our instructions.

Standard Contractual Clauses or **SCCs** means the standard contractual clauses approved by the European Commission under Commission Implementing Decision (EU) 2021/914 of 4 June 2021.

UK Addendum means the addendum to the SCCs approved by the UK Information Commissioner.

2. Roles and responsibilities of the parties

2.1 You are the controller of Personal Information. We are the processor (as defined in the GDPR or other Applicable Data Privacy Laws) or service provider (as defined under the CCPA or other Applicable Data Privacy Laws) and Process Personal Information on your behalf and subject to your instructions. Unless otherwise expressly indicated, if you are subject to Applicable Data Privacy Laws in the United States, we Process Personal Information relating to students as a "School Official" performing an outsourced institutional function, pursuant to FERPA 34 CFR Part 99.31(a)(1). You (and/or your Authorized Users) are the owner of Personal Information: When we Process Personal Information on your behalf, you retain all right, title and interest to such Personal Information and Anthology does not own, control, or license such information except as described in the Agreement.

2.2 To the extent Applicable Privacy Laws such as the GDPR require a description of the subject matter, scope, duration, nature and purpose of the Processing of Personal Information, including the type of Personal Information and categories of data subjects, the descriptions set out in the Agreement and Annex A of this DPA apply. You have entered into the Agreement with us to benefit from our expertise in Processing Personal Information solely for the purposes set out herein and in the Agreement. We shall be allowed to exercise our own discretion in the selection and use of means as we consider necessary to pursue those purposes, subject to the requirements of this DPA and Applicable Data Privacy Laws.

3. Our obligations

3.1 Anthology (together with its employees, affiliates, and subsidiaries), may Process the Personal Information as a service provider and, in doing so, may retain, use, disclose and otherwise Process Personal Information solely in accordance with your instructions and for the following purposes: (i) providing Products and Services to you including any functionalities activated by your system administrators, (ii) updating and enhancing the functionalities of the Products and Services; (iii) maintaining and supporting our Products and Services; (iv) as otherwise permitted or required by Applicable Data Privacy Laws. We may also Process Personal Information as necessary to enforce our rights under the Agreement. Without limiting the foregoing, we will not:

(a) retain, use, or disclose Personal Information for any purpose other than for the business purposes specified in the Agreement or the DPA or as otherwise permitted by Applicable Data Protection Laws; or

(b) retain, use, or disclose Personal Information outside of our direct business relationship with you; unless expressly permitted by the Applicable Data Protection Laws.

3.2 The Agreement and the DPA along with your configuration of the Products and Services are your instructions to us in relation to the Processing of Personal Information. We agree to follow such instructions with regard to the Processing of Personal Information. Our obligations under Sections 3.1 and this 3.2 shall be subject to Section 4.2.

3.3 Provided that we Process only the minimum amount of Personal Information necessary, and the output of the Processing is aggregated or De-Identified Data (to which we implement appropriate technical

safeguards and businesses processes to prevent the re-identification of individuals), you agree that we may Process Personal Information for additional lawful purposes, including: (i) evaluating, improving and/or developing our Products and Services; (ii) developing new Products and Services; and (iii) analytics and research. We may suggest supplemental educational tools or services to Authorized Users to the extent consistent with Applicable Data Privacy Laws; however, we will not use Personal Information for targeted advertising, without the consent of you or your Authorized Users.

3.4 You acknowledge that where we Process personal information: (i) in the context of a direct relationship we have with an Authorized User in the course of providing or offering services to them; or (ii) with the consent of an Authorized User solely with respect to their own personal information, our Processing activities are outside the scope of this DPA. You agree to Anthology's fulfilment of any legally satisfactory request and consent by an Authorized User to download, export, save, maintain, or transfer their own personal information.

3.5 In the unlikely event that applicable law or legal process requires us to Process Personal Information other than as instructed, we will notify you unless prohibited from so doing by applicable law.

3.6 We agree to uphold our responsibilities under Applicable Data Privacy Laws and to supervise and train our employees accordingly. We will ensure that such persons with access to Personal Information have a business need to access the Personal Information and have committed themselves to confidentiality (or are under an appropriate statutory obligation of confidentiality.

3.7 If we receive a request for disclosure of Personal Information by a law enforcement authority or other organization or body, we will:

(a) refer the requesting authority to you where legally permissible;

(b) promptly notify you prior to the compelled disclosure unless legally prohibited;

(c) if we are prohibited from notifying you, use our best efforts to obtain a waiver of the prohibition and otherwise take reasonable steps to notify you after the prohibition expires;

(d) ensure that the request is legally binding and valid;

(e) try to challenge the request and seek interim measures where we believe a request is invalid or unlawful, with a view to suspending the effects of the request until the competent judicial authority has decided on its merits; and

(f) interpret requests narrowly and provide only the minimum amount of information permissible to comply with the request.

3.8 If, and to the extent, that we receive De-Identified Data from you, then we will take the following measures except as otherwise instructed by you:

(a) take reasonable measures to ensure the information cannot be associated with an individual.

(b) publicly commit to Process the De-Identified Data solely in deidentified form and not to attempt to reidentify the information.

(c) Contractually obligate any recipients of the De-Identified Data to comply with the foregoing requirements and Applicable Data Protection Laws.

4. Your obligations

4.1 You warrant your collection and sharing of Personal Information with us shall comply with Applicable Data Privacy Laws.

4.2 You warrant that you will give only lawful instructions. If we hold the view that any instruction of yours contravenes Applicable Data Privacy Laws and/or the DPA, we will notify you, and we are entitled to suspend execution of the instruction, until you confirm such instruction in writing. We have the right to deny the execution of an instruction – even if issued in writing – in case we conclude that we would be liable under Applicable Data Privacy Laws if we execute the instructions you have provided.

4.3 You represent and warrant that:

(a) you have the authority to provide Personal Information to Anthology, or to permit Anthology to collect directly, for its use in accordance with the Agreement; and

(b) you have obtained and provided all required consents and/or disclosures to Authorized Users regarding Anthology's collection, access, transfer, and Processing of Personal Information under this Agreement, including to the extent applicable, to permit Anthology to collect Personal Information directly from students under age thirteen (13) as permitted under the Children's Online Privacy and Protection Act ("COPPA").

(c) Except for our Products and Services that specifically require or allow for such data, you will not use the Products and Services to Process any data subject to the Payment Card Industry Data Security Standards ("PCI DSS"), Protected Health Information (PHI) or other legally protected types of data that require standard and controls exceeding the standards and controls described in this DPA.

4.4 To the extent necessary to provide you with the Products and Services, you authorize us, our affiliates, and subsidiaries to Process Personal Information and you will facilitate a reasonable method for us to obtain such information, for example via secure transfer from and/or authorized access to your student information systems.

4.5 Where Anthology discloses our employees' or contractors' Personal Information to you or an Anthology employee/contractor provides their Personal Information directly to you, which you Process to manage your use of the Products and Services, you will Process that Personal Information in accordance with your data privacy policies and Applicable Data Privacy Laws. We will only make such disclosures where lawful for the purposes of managing your use of the Products and Services.

5. Cooperation

5.1 We will, to the extent legally permitted, promptly notify you if we receive an Individual Right Request or redirect such a request to you. Our response to an individual Right Request will be limited to explaining to the individual that the Individual Right Request needs to be addressed to you.

5.2 If you do not have the ability to address an Individual Right Request directly through our Products and Services, we will upon your request assist you in responding to the Individual Right Request for the fulfilment of your obligation under Applicable Data Privacy Laws.

5.3 Unless legally prohibited, we will make available to you any information you request and otherwise reasonably assist you as necessary to demonstrate compliance with your obligations under Applicable Data Privacy Laws in relation to Personal Information (including obligations under Art. 32 to 36 GDPR).

6. Third Party Access (Sub-processors)

6.1 We shall not disclose, release or otherwise transfer Personal Information to any third party without consent from you or an Authorized User, except where such disclosure is permitted (i) to a Sub-processor that Processes Personal Information on our behalf in support of Anthology's Processing of Personal Information in accordance with Section 3.1 or 3.2, (ii) to a third party as reasonably necessary to comply with any applicable law, regulation, or public authority, (iii) to respond or participate in judicial process or

to protect the safety of Anthology or our users, or (iv) as otherwise permitted by Applicable Privacy Laws. Without limiting the foregoing, we will not:

(a) sell Personal Information or otherwise making Personal Information available to any third party for monetary or other valuable consideration, other than a transfer in the context of a merger, acquisition or other business transaction involving the sale of all or part of the business;

(b) share Personal Information with any third party for cross-context behavioral advertising.

6.2 The lists of Anthology's current Sub-processors are available at *https://help.blackboard.com/subprocessors* (for products formerly provided as "Blackboard") and *https://help.blackboard.com/Anthologysubprocessors* (for product formerly provided as "Anthology"). Subject to Section 6.3, you hereby give us a general authorization to engage the Sub-processors listed at these links.

6.3 We shall:

(a) inform you of any intended changes concerning the addition or replacement of Sub-processors at the link in Section 6.2 above (in combination with our email notification mechanism available at the links for which you will need to register to receive notifications) thirty (30) days prior to any changes; and

(b) give you the opportunity to raise reasonable objections to such changes within twenty (20) calendar days of such notification. We may add or replace a Sub-processor immediately if it is necessary to ensure business continuity and recovery in case of emergency, except as prohibited by Applicable Data Privacy Laws.

6.4 With regard to our Sub-processors we will:

(a) conduct due diligence on the data privacy and security measures of new Sub-processors before providing access to Personal Information;

(b) enter into a written agreement which requires at least the same level of protection for Personal Information and individuals as set out in this DPA before providing access to Personal Information;

(c) restrict the Sub-processor's access to Personal Information only to what is necessary to fulfil our contractual obligations or as otherwise permitted under the Agreement or under Applicable Data Privacy Laws; and

(d) remain liable for any Processing of Personal Information carried out by Sub-processors to the same extent we would be liable if performing the Services ourselves.

7. Customer-Requested Third-Party Access (Third Party Integrations)

7.1 Some of our Products and Services provide for or allow for integrations with third parties products and services. Enabling an integration with the product or service of a third party acting on your behalf and under your instruction ("Third Party Data Processor") by you or your Authorized User within our Products and Services, is considered your authorization and instruction to interact with and exchange the necessary Personal Information with the Third Party Data Processor. You agree that if and to the extent such exchanges of Personal Information occur, between you and us, you are responsible for (i) ensuring that such exchanges are lawful, (ii) the consequences of exchanging the Personal Information to the Third-Party Data Processor, and (ii) entering into separate contractual arrangements with such Third-Party Data Processors binding them to comply with obligations in accordance with Applicable Data Privacy Laws. For the avoidance of doubt, such Third-Party Data Processors are not our Sub-processors.

8. **Personal Information Hosting and Access**

8.1 Generally, Anthology has a regional hosting model. For example, in the United States, all Personal Information is hosted on servers in the United States. For the delivery of the Products and Services, support, development, maintenance and similar purposes, your Personal Information may be Processed outside of the country in which it was originally collected.

8.2 If your Products and Services are not hosted regionally, you acknowledge and agree that to deliver the Products and Services and for support, development, maintenance and similar purposes, Personal Information may be Processed in countries other than the country in which it was collected. However, we will not Process Personal Information outside of the country it was collected unless such access meets the requirements under Applicable Data Privacy Laws. For sake of clarity, regardless of where we Process Personal Information, all Processing will be carried out in accordance with this DPA.

9. **Personal Information Transfers**

9.1 We will comply with all requirements regarding transfers of Personal Information directly applicable to us which do not require your cooperation. If applicable requirements regarding transfers of Personal Information require your cooperation, we will take such steps with you as required or permitted to comply with these requirements.

9.2 If you are located in the EEA or the UK, we will not transfer Personal Information to any country outside the EEA or the UK which has not been the subject of a adequacy decision unless we have ensured that such a transfer adequately protects Personal Information and is made pursuant to an appropriate legal transfer mechanism, such as the P2P SCCs, Binding Corporate Rules approved by the European Data Protection Board, or any other legal transfer mechanism.

9.3 Notwithstanding the provisions of paragraph 9.2 above, you agree that Personal Information may need to be transferred to Anthology group companies and third-party Sub-processors outside the EEA and the UK, in order for one or more of those entities to assist with our provision of Products and Services to you. In respect of such transfers, Anthology has implemented an intra-group data transfer agreement based on the P2P SCCs, incorporates P2P SCCs with its third party Sub-processors as required, and has implemented supplementary measures to help ensure that personal information is adequately protected when transferred.

9.4 If you are subject to the relevant UK and/or EEA data transfer requirements despite being located outside the EEA or the UK, the following applies;

(a) If the Anthology entity listed in the Master Agreement or order form is located in the EU or the UK, Section 9.2 and 9.3 above apply (notwithstanding that you are located outside the EEA or the UK).

(b) If the Anthology entity listed in the Master Agreement or order form is located outside the EU or UK, Section 9.2 and 9.3 are disapplied and the parties agree that the C2P SCCs are expressly incorporated into this DPA in accordance with Part 1 of Annex C. Further, where the applicable transfers are subject to UK data transfer requirements specifically, such C2P SCCs shall be deemed to be amended by the UK Addendum which shall also be expressly incorporated into this DPA in accordance with Part 2 of Annex C.

9.5 To the extent that the P2P SCCs or C2P SCCs and/or the UK Addendum are declared invalid (by, for example, a competent court or authority), we will implement an alternative legal transfer mechanism.

10. **Security**

10.1 We will implement commercially reasonable technical and organizational measures to ensure an appropriate level of security to protect including Personal Information. Annex B describes our technical

and organizational security measures. The security measures are subject to technological advancements and further development. We are permitted to implement suitable alternative measures, as long as the alternative measures do not materially decrease the level of security applied to the Personal Information and meet the requirements of Applicable Data Privacy Laws.

10.2 We will regularly audit and assess our compliance with the technical and organizational security measures.

10.3 You are responsible for the appropriate use of the security features and other features of our Products and Services by you and your Authorized Users, including the granting and management of access entitlements. You are responsible for determining whether our Products and Services (including any test and staging environments) and the related security measures are sufficient for the intended Processing of Personal Information before using these Products and Services. We will provide you with any information that is reasonably required to make this determination. If you use one of our Products and Services that require you to schedule and install updates, you are responsible for ensuring that you promptly install any recommended updates once available and that you use the recommended most recent versions of our Products and Services.

11. **Security Incident**

11.1 Anthology maintains a documented security incident response plan which is regularly tested.

11.2 Upon becoming aware of a Security Incident, we will (i) promptly investigate such Security Incident in accordance with our security incident response plan, (ii) take all measures and actions as are reasonably necessary to remedy or mitigate the effects of such Security Incident, and (iii) notify you promptly and without undue delay (and in any event within the time period required by applicable law) in writing upon confirmation of a Security Incident involving the unauthorized access, acquisition or disclosure of Personal Information that compromises the security, confidentiality or integrity of the Personal Information or as otherwise required by Applicable Data Privacy Laws ("Confirmed Security Incident").

11.3 In the event of a Confirmed Security Incident, we will:

(a) provide timely cooperation and assistance as you may require to fulfil your Security Incident reporting obligations under Applicable Data Privacy Laws.

(b) assist you in relation to any Security Incident notifications you may be required to make under applicable law. To the extent such information is available and required by law, the notification under Section 11.2 shall include the following:

(i) a general description of the Security Incident, including the nature and date of the Security Incident;

(ii) the categories and approximate number of individuals concerned;

(iii) the categories and approximate number of Personal Information records concerned;

(iv) the likely consequences of the Security Incident;

(v) the measures used to protect the Personal Information;

(vi) the measures we have taken or propose to take to address the Security Incident, including, where appropriate, measures to mitigate its possible adverse effects; and

(vii) the name and contact details of our relevant point of contact with regard to the Security Incident.

(c) Upon request, provide reasonably requested information about the status of any Anthology remediation and restoration activities and keep you informed about all material developments in connection with the Security Incident.

11.4 In the event of a Confirmed Security Incident, you will be responsible for the timing, content, and delivery of any legally required notification to your Authorized Users who are impacted by such Confirmed Security Incident and to any regulator or third party in accordance with applicable law. If, due to a Confirmed Security Incident which results from a breach of the data security obligations set forth in Annex B by Anthology, its agents, or Sub-processors acting on its behalf, any third-party notification is required under applicable law, Anthology shall, subject to the limitations of liability in the Agreement, reimburse you for all reasonable "Notification Related Costs." Notification Related Costs are limited to internal and external costs associated with addressing and responding to the Confirmed Security Incident, including but not limited to: (a) preparation and mailing or other transmission of notifications required by applicable law; (b) establishment of an adequate call center and other communications procedures in response to the Confirmed Security Incident; (c) costs for remediation measures such as credit monitoring or reporting services for affected individuals for at least twelve (12) months in relation to a Security Incident that involves social security numbers, or to the extent required by law. With respect to any Security Incident which does not result from a breach of the data security obligations set forth in Annex B by Anthology, its agents, or Sub-processors acting on its behalf, any third-party notifications, if any, shall be at your expense.

11.5 Anthology's obligation to report or respond to a Confirmed Security Incident under this Section 11 is not and will not be construed as an acknowledgement by Anthology of any fault or liability of Anthology with respect to the Confirmed Security Incident.

11.6 Unless prohibited by law, you will notify us before communicating the Confirmed Security Incident to a third party (whether to any regulators, Authorized Users, clients, or the public) and provide us with copies of any written documentation to be filed with the regulators and of any other notification you propose to make which references us, our security measures and/or role in the Confirmed Security Incident, whether or not by name. Subject to your obligations to comply with any mandatory notification deadlines under Applicable Data Privacy Laws, you will consult with us in good faith and take account of any clarifications or corrections we reasonably request to such notifications or communications, and which are consistent with Applicable Data Privacy Laws.

12. **Audit**

12.1 We will, by way of regular internal or external audits, verify that the Processing of Personal Information complies with Applicable Data Privacy Laws.

12.2 Subject to Sections 12.3 -12.5, we will allow for and contribute to audits, including inspections, conducted by you or another auditor mandated by you regarding our compliance with the DPA and Applicable Data Privacy Laws.

12.3 To fulfil our obligations under 12.2, we will provide you, upon request, appropriate documentation to assist you with your audit obligations, including (and as available), Higher Education Community Vendor Assessment Toolkit (HECVAT) reports, ISO certification documents, and SOC 2 reports.

12.4 If, after review of the documentation provided in accordance with Section 12.3, you require further information to meet your obligations under Applicable Data Privacy Laws, you may request further information with an explanation regarding what further information is required and why it is required.

12.5 If after review of the additional documentation provided in accordance with Section 12.4, you still require further information to meet your obligations under Applicable Data Privacy Laws, you may no more once per year, request an audit where Applicable Data Privacy Laws grant you the right to conduct an audit.

12.6 You will reimburse us for reasonable expenses for any time expended for the audits conducted in accordance with Section 12.5. Requests need to be made at least fourteen (14) days in advance in writing, and we will mutually agree upon the scope, timing, and duration of the audit and the execution of an appropriate confidentiality agreement.

12.7 Any information made available in accordance with this Section 12 shall be deemed Confidential Information. Upon request, you will provide us with a copy of any audit reports produced in relation to audits conducted under this section, unless prohibited by applicable law. You will promptly notify us regarding any possible non-compliance discovered during the course of an audit, and we will use commercially reasonable efforts to address any confirmed non-compliance as soon as practicable.

13. Deletion or return of Personal Information

13.1 Upon expiration or termination of the Products or Services, or such earlier time upon request, we will delete the relevant Personal Information in our possession, custody or control within a reasonable time and procure the deletion of all copies of Personal Information processed or maintained by any Sub-processors. At your request and your expense, we will return such Personal Information to you before deleting it, provided that a request for the return of Personal Information is submitted to Anthology in writing at least thirty (30) days prior to the date of termination. If no such request for the return of Personal Information is received, Anthology may, but shall have no obligation to, maintain or return Personal Information more than 10 days after the termination of the Products or Services. We will certify the deletion of Personal Information upon request.

13.2 Notwithstanding the foregoing, we may retain Personal Information to the extent: (i) required by applicable laws; (ii) required as part of our automated backup and recovery processes so long as the backup and recovery storage system is inaccessible to the public, Processing is limited to back-up and recovery purposes and governed by the protection of this DPA; (iii) an Authorized User has downloaded, saved, transferred or otherwise maintained their own personal information in a personal account in accordance with Section 4.3; and/or (iv) it is aggregated or De-Identified Data and Anthology has implemented technical safeguards and business processes to prohibit the reidentification of the information with an individual. If you request deletion of Personal Information in archival and back-up-files, you shall bear the costs including costs for business interruptions associated with such request.

14. Final provisions

14.1 Unless specifically stipulated to the contrary by the Parties, the duration of this DPA will be coterminous with the term of the Agreement. Our obligations under the DPA will continue to apply as long as we Process Personal Information.

14.2 This DPA is incorporated into and made a part of the Agreement by this reference and replaces any arrangements agreed earlier between the parties in respect of the Processing of Personal Information related to the Agreement. In the event of a conflict between this DPA and any other provision of the Agreement between you and us, this DPA will prevail; provided that if you and we have agreed in an Order Form to any terms that are different from this DPA, the terms in such Order Form will prevail. Notwithstanding the foregoing, in the event of a conflict between: (a) the DPA; (b) any provision of the Agreement; or (c) the Order Form, and the SCCs, the SCCs shall prevail.

14.3 Notwithstanding any notice requirements in the Agreement, we may update this DPA from time to time to better reflect changes to the law, new regulatory requirements or improvement to the Products and Services. The updated Terms shall be posted here: http://agreements.blackboard.com/bbinc/data-processing-addendum.aspx. If any update to the DPA constitutes a material change to the ways in which we Process Personal Information, or materially affects your use of the Products and Services or your rights herein, we will provide you with reasonable notice prior to the changes taking effect. Your continued use of the Service thereafter shall constitute acceptance to be bound by the updated DPA.

Annex A – Details of Processing

This Annex A describes the Processing of Personal Information as required under some Applicable Data Privacy Laws such as GDPR.

The details of the Processing depend on your use of our Products and Services but will typically be as follows:

Categories of Personal Information

- Name or unique identifiers
- Personal contact information and information about role at institution
- Date of birth, gender, parent or guardian/student relationships
- Access credentials such as usernames and passwords, profile settings, language information
- Information related to the devices accessing our Products and Services, service or browsing history, location data
- Information provided by social networks (only where Customer enables integrations with social networks),
- Admissions and enrolment information
- Course and degree information such as grade level, teachers, classes/sections/courses, grades, assignments, tests, books, attendance, homework, degree type
- Personal information contained in content generated and/or provided by an Authorized User such as submitted papers, assignments, blog and discussion posts, messages sent within Products and Services contributions to online collaboration such as chats and audio/video conferencing
- Information about non-curricular groups and activities
- For Products and Services supporting the management of financial aid only: Financial information, tax information, information about eligibility for financial aid, last 4 digits of Social Security Number, and other information necessary for the management of financial aid
- For Products and Services supporting alumni management: Donation tracking, gift processing and other information required for the management of alumni and donations
- For Anthology Finance & Human Capital only: Personal Information related to recruitment and management of staff including performance and compensation information
- For Anthology Payroll only: Staff compensation, bank account and other information required for payroll management
- For Anthology Encompass only: Credit card transactions and information
- Reporting and analytics information including predictive analytics based on the above data categories
- If the definition of Personal Information under Applicable Data Privacy Laws such as POPIA includes information about juristic persons: Company registration information, contact details of authorized representatives, registered address, applicable tax numbers, financial information, relevant registrations, and other information which may be relevant to our engagement with you

Special Categories of Personal Information (if any)

Our Products and Services are generally not intended to Process Special Categories of Personal Information. Any Processing of Special Categories of Personal Information is determined and controlled by you in compliance with Applicable Data Privacy Laws.

Special Categories of Personal Information may include: (a) Personal Information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; (b) genetic data and biometric data Processed for the purpose of uniquely identifying an individual; and (c) data concerning health or data concerning an individual's sex life or sexual orientation.

Categories of Data Subjects

Customer’s representatives (such as employees, contractors, consultants, and agents) and Customer’s constituents (such as students, prospective students, alumni, donors, parents, teachers, administrators, guest users invited by Customer or its Authorized Users, and other Authorized Users.

Subject matter, purpose and nature of Processing

As a provider of education technology solutions, we Process Personal Information provided by you or your Authorized End Users on your behalf and under your instructions within the scope of the Agreement. Processing operations may include storage and other Processing necessary to provide our Products and Services and otherwise perform our obligations as described in Section 3.

Duration of Processing

We will Process Personal Information for the period permitted under the Agreement, or until you direct us to return or delete it in accordance with the DPA.

Annex B – Security Measures

We use the following appropriate technical and organizational measures to protect Personal Information which have to meet, at a minimum, the level required by Applicable Data Privacy Laws:

Management controls

- We maintain a comprehensive information security program with an appropriate governance structure (including a dedicated Information Security team) and written security policies to oversee and manage risks related to the confidentiality, availability, and integrity of Personal Information.

- We align our information security program and measures with industry best practices, such as the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27001, Open Web Application Security Project (OWASP), and National Institute of Standards and Technology (NIST) 800 frameworks. These controls are distilled and incorporated into an internal compliance framework that is applicable to all Products and Services.

- We use internal resources and third-party contractors to perform audits and vulnerability assessments and provide guidance on best practices for select systems containing Personal Information. System assessments and network audits are performed regularly. Issues identified during audits are prioritized and remediated as part of ongoing security monitoring using a risk management methodology.

- Our employees receive security and data privacy training when they start and annually thereafter. Awareness campaigns are used to raise awareness about information security risks and our information security policies and procedures. Select staff, such as developers, receive additional security training tailored to their job role. Completion of training is tracked.

- New employees undergo background checks prior to onboarding, where permitted by applicable law, and sign a confidentiality agreement.

- Employees are required to comply with internal policies on the acceptable use of corporate IT assets. These policies address requirements on clean desk and secure workspaces, protecting system resources and electronic communications, protecting information, and general use of technology assets. Our employees are made aware that non-compliance with these policies can lead to disciplinary action, up to and including termination of employment/contract.

- We maintain a vendor risk management program to manage the security and integrity of our supply chain. Our procurement process for third party service providers that have access to confidential information (including Personal Information) includes a vendor security and privacy assessment review and a contract review by our Legal team.

- We have a documented security incident response process for responding to, documenting, and mitigating Security Incidents and notifying our clients, authorities or other parties as required. The process is reviewed and tested regularly.

Admission control

- We employ appropriate physical safeguards to prevent unauthorized persons from gaining access to the premises where Personal Information is collected, processed, and used. Such premises may only be entered by us and/or our agents.

- We and our service providers implement physical security controls for the data centers used to store Personal Information. These controls are commensurate with industry best practices and local regulations, which include 24x7x365 video monitoring, guards, secured ingress/egress, badged access, sign-in/sign-out logs, restricted access, and other best practices.

- We use appropriate measures to secure buildings, such as using access cards or fobs for employee access.

- We use appropriate measures to ensure that Personal Information held in hardcopy are kept securely e.g., in locked rooms or filing cabinet. Generally, steps are taken to ensure that access to hardcopy Personal Information is limited in the same way it would be on an electronic IT system, i.e., access is limited to those individuals where it is necessary for them to have access in order for them to perform their job role.

Entry control

- We use appropriate measures to prevent unauthorized parties from accessing or using our systems containing Personal Information.

- We require authentication and authorization to gain access to systems that Process Personal Information (i.e., require users to enter a user id and password before they are permitted access to such systems).

- We have procedures in place to permit only authorized persons to access Personal Information internally or externally by using authentication procedures (e.g., by means of appropriate passwords), except as otherwise enabled by you.

Access control

- We employ appropriate measures to prevent individuals accessing Personal Information unless they hold a specific access authorization.

- We only permit access to Personal Information which the employee (or agent) needs for his/her job role or the purpose they are given access to our systems for (i.e., we implement measures to ensure least privilege access to systems that Process Personal Information). System administration and privileged access is controlled and enforced on a need-to-know basis and is reviewed regularly.

- We have in place appropriate procedures for controlling the allocation and revocation of access rights to Personal Information. For example, having in place appropriate procedures for revoking employee access to systems that Process Personal Information when they leave their job or change role. Unnecessary and default user accounts and passwords are disabled on servers.

- Our systems containing Personal Information are protected by user identifiers, passwords, and role-based access rights. Special access rights are produced for the purposes of technical maintenance which do not allow access to Personal Information.

- We implement methods to provide audit logging to establish accountability by monitoring network devices, servers, and applications. Where applicable, aberrant activity generates alerts for investigation and/or action.

- All employees must use multi-factor authentication for remote access to IT assets within the corporate network.

- We take appropriate administrative safeguards to protect our services against external attacks, including, for example, deploying firewalls and using services to provide 24x7x365 security monitoring of our data centers to protect and defend against external security threats.

Transmission control

- We encrypt Personal Information while in transit over the internet to preserve its confidentiality and integrity.

Input control

- We maintain logging and auditing systems to monitor activity related to the input of Personal Information.

Order control

- We ensure that all requests from you with respect to Personal Information are processed strictly in compliance with your instructions through the use of clear and unambiguous contract terms; comprehensive Statements of Work; appropriately designed policies and processes, and training.

Availability control

- We protect Personal Information in our possession against unintentional destruction or loss by implementing appropriate management, operations, and technical controls such as firewalls; monitoring; and backup procedures.

- Example measures that may also be taken include mirroring of storage media, uninterruptible power supply (UPS); remote storage; and disaster recovery plans.

Annex C (C2P SCCs and UK Addendum for Clients Located Outside the EEA or the UK)

Part 1 - C2P SCCs

In relation to the C2P SCCs incorporated in accordance with Section 9.4,

(a) the optional clause 7 (docking clause) is not used;

(b) for clause 9(a), option 2 (general written authorization) is selected and the specified time period is thirty (30) days;

(c) the optional language at clause 11(a) (redress) is not used;

(d) for clause 13(a), the first optional paragraph is used;

(e) for clause 17, the selected governing law shall be the law of the Netherlands;

(f) for clause 18(b), the selected forum shall be the courts of the Netherlands;

(g) for Annex I, Part A:

(i) the data exporter is you and the data importer is the Anthology group entity listed in the Master Agreement and/or relevant order form;

(ii) the data exporter's, and data importer's, name and address, and the contact person's contact details, shall be those specified in the Master Agreement and/or relevant order form, and the contact person shall be the respective signatories to the Master Agreement and/or relevant order form;

(iii) the activities relevant to the data transferred under these Clauses shall be: the data exporter has entered into the Master Agreement with the data importer for the provision of the Products and Services (as defined in the Master Agreement), and the data importer provides the Services in accordance with the Master Agreement, order form and this DPA; and

(iv) the Parties agree that the signature of the Master Agreement and/or relevant order form shall constitute execution of the C2P SCCs, on the date of the Master Agreement and/or relevant order form.

(h) for Annex I, Part B:

(i) the categories of data subjects, categories of personal data sensitive data transferred, and the purpose and nature of the process shall be as specified in Annex A to this DPA;

(ii) the frequency of the transfer shall be ongoing until the personal data is deleted in accordance with the Agreement and the DPA; and

(iii) the period for which the personal data will be retained shall be in accordance with the terms of the Agreement and the DPA

(i) for Annex I, Part C, the competent supervisory authority shall be the Dutch Data Protection Authority;

(j) for Annex II, the technical and organizational security measures shall be those specified in Annex B to this DPA; and

(k) for Annex III the authorized sub-processors are those listed at the links available in Section 6.2 in of the DPA.

Part 2 – UK Addendum

In relation to the UK Addendum incorporated in accordance with Section 9.4:

(a) For Table 1:

(i) The start date shall be the date of the Master Agreement and/or the relevant order form;

(ii) The parties' details shall be as specified in the incorporated C2P SCCs;

(iii) The key contact details shall be that of the signatory to the Master Agreement and/or the relevant order form;

(iv) the Parties agree that the signature of the Master Agreement and/or relevant order form shall constitute execution of the UK Addendum, on the date of the Master Agreement and/or relevant order form.

(b) For Table 2, the first option shall be deemed selected.

(c) For Table 3, the details to be included shall be those set out in the incorporated C2P SCCs.

(d) For Table 4, neither Party is selected.