Data Processing Addendum

Last published: ***8/10/2026***

This Data Processing Addendum (**"DPA"**) is entered into by and between **Student First, Inc.**, a Delaware corporation (**"Student First"**), and the customer identified in the Agreement (**"Customer"** and, together with Student First, the **"Parties"** and each a **"Party"**). This DPA is incorporated into and forms part of the Master Services Agreement or other written or electronic agreement between the Parties governing Customer's access to and use of the Services (the **"Agreement"**). This DPA is effective as of the effective date of the Agreement.

Purpose. Student First provides a cloud-based student information system and related services to institutions of higher education. In providing the Services, Student First Processes Personal Data on behalf of and under the instructions of Customer. This DPA sets out the Parties' respective obligations with respect to such Processing and is intended to satisfy the requirements of Applicable Data Protection Laws. Except as expressly modified here, the Agreement remains in full force and effect.

1. **DEFINITIONS**

    1. Capitalized terms used but not defined in this DPA have the meanings given in the Agreement. For purposes of this DPA:

        "Applicable Data Protection Laws" means all laws and regulations applicable to the Processing of Personal Data under this DPA, including, to the extent applicable to a given Party and a given Processing activity: (a) the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g, and its implementing regulations at 34 C.F.R. Part 99 (**"FERPA"**); (b) the Gramm-Leach-Bliley Act and the Federal Trade Commission Standards for Safeguarding Customer Information, 16C.F.R. Part 314 (the **"Safeguards Rule"**); (c) the Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506 (**"COPPA"**); (d) state privacy, data protection, and data breach notification laws applicable to the Personal Data, including the California Consumer Privacy Act, as amended (the **"CCPA"**),and comparable comprehensive state privacy statutes. Subject to Sections 15.3 and 15.5 and to the extent the parties enter into an International Addendum, Applicable Data Protection Laws includes, as identified in the International Addendum, the EU General Data Protection Regulation 2016/679 (**"GDPR"**), the UK GDPR and Data Protection Act 2018, and Canadian federal or provincial privacy laws.

        "Data Subject" means an identified or identifiable natural person to whom Personal Data relates, including students, applicants, prospective students, parents and guardians, and Customer's personnel whose Personal Data is Processed under the Agreement.

        "De-Identified Data" means information that was derived from Personal Data but that has been processed so that it meets the standard set out in Section 14 (De-Identified Data).

”Education Records” means education records” as defined under FERPA and its implementing regulations, to the extent Processed by Student First under the Agreement.

”Personal Data” means any information Processed by Student First on behalf of Customer under the Agreement that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular Data Subject or household, including Education Records and “personally identifiable information” as defined under FERPA. Personal Data does not include De-Identified Data.

”Process” means or “Processing” means any operation performed on Personal Data, whether or not by automated means, including collection, recording, organization, structuring, storage, adaptation, retrieval, consultation, use, disclosure, dissemination, alignment, combination, restriction, erasure, or destruction.

”Security Incident” means a breach of Student First’s security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to Personal Data Processed by Student First or its Subprocessors. A Security Incident does not include an unsuccessful attempt or activity that does not compromise the security of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial-of-service attacks, and other network attacks on firewalls or networked systems, or the introduction of malware that is quarantined or otherwise prevented from accessing Personal Data.

”Services” means the student information system, financial aid, and related services made available by Student First under the Agreement.

”Subprocessor” means any third party engaged by Student First to Process Personal Data on Student First’s behalf in connection with the Services, including infrastructure and hosting providers.

Role-based terms. Where the context or Applicable Data Protection Law requires, **“controller,” “processor,” “business,” “service provider,” “sell,” “share,”** and **“personal information”** have the meanings given under the applicable statute (for example, the GDPR or the CCPA), and are applied to the Parties in the roles described in Section 2.

2. **ROLES OF THE PARTIES; SCOPE**

1. **Customer as controller.** As between the Parties, Customer is the controller and “business” with respect to Personal Data and determines the purposes and means of its Processing. Customer is responsible for the accuracy, quality, and lawfulness of Personal Data and for having provided all notices and obtained all rights, consents, and authorizations necessary for Student First to Process Personal Data as contemplated by the Agreement and this DPA.
2. **Student First as processor / service provider.** Student First is a processor and “service provider” that Processes Personal Data solely on behalf of, and in accordance with the documented instructions of, Customer. The Agreement, this DPA, Exhibit A (Details of Processing), and

Customer's configuration of and use of the Services constitute Customer's complete and documented instructions. Student First will not Process Personal Data for any purpose other than performing the Services and its obligations under the Agreement, except (a) as expressly permitted for De-Identified Data under **Section 14**, (b) where required by law, in which case Student First will, unless legally prohibited, inform Customer of the legal requirement before Processing, and (c) as requested by Customer.

3. **Service provider restrictions (CCPA and comparable laws).** Student First will not: (a) sell or share Personal Data; (b) retain, use, or disclose Personal Data for any purpose other than the business purposes specified in the Agreement, including outside the direct business relationship between the Parties; or (c) combine Personal Data with personal information Student First receives from or on behalf of another person, or collects from its own interaction with a Data Subject, except as permitted under Applicable Data Protection Law to perform a business purpose. Student First understands the restrictions in this Section and will comply with them, and will notify Customer if it determines it can no longer meet its obligations under Applicable Data Protection Law. The Parties acknowledge that the disclosure of Personal Data by Customer to Student First is not a sale and is made only to enable Student First to perform the Services.
4. **Details of Processing.** The subject matter, duration, nature and purpose of the Processing, the categories of Personal Data and Data Subjects, and the frequency of Processing are set out in Exhibit A.

3. **FERPA COMPLIANCE**

1. This Section applies to the extent Customer is an educational agency or institution subject to FERPA and Student First Processes Education Records on Customer's behalf.
2. **School official designation.** Customer designates Student First as a "school official" with a "legitimate educational interest" in the Education Records to which Student First is provided access, within the meaning of 34 C.F.R. §§ 99.31(a)(1) and 99.7(a)(3)(iii). Student First (a) performs an institutional service or function for which Customer would otherwise use its own employees; (b) is underthe direct control of Customer with respect to the use and maintenance of Education Records; and (c) is subject to the requirements of 34 C.F.R. §99.33(a) governing the use and redisclosure of personally identifiable information from Education Records. Customer represents that it has provided any notices required under FERPA to designate Student First as a school official.
3. **Use and redisclosure.** Student First will use Education Records only to provide the Services and for no other purpose, and will not redisclose personally identifiable information from Education Records to any third party except (a) to Subprocessors engaged in accordance with Section 8 and bound to equivalent restrictions, (b) as authorized in writing by Customer, or (c) as required by law, in which case Student First will, unless legally prohibited, notify Customer before disclosure. Student First will not use Education Records to engage in targeted advertising to Data Subjects.
4. **Direct control; access.** Student First will maintain Education Records only as necessary to provide the Services and in accordance with Customer's documented instructions, including Customer's configuration and use of the Services. Customer may use the functionality of the Services to access, review, correct, amend, export, ordelete Education Records as needed to comply with FERPA. Where Customer cannot reasonably fulfill a FERPA access or amendment request through the Services,

Student First will provide reasonable assistance at Customer's direction and subject to the Agreement.

5. **Recordkeeping.** Customer is responsible for maintaining any record of disclosures required under FERPA. To the extent disclosures of Education Records are made by or through the Services and the relevant information is reasonably available to Student First, Student First will provide reasonable assistance to Customer, upon request, to support Customer's FERPA record keeping obligations.

4. **FINANCIAL AID DATA; SAFEGUARDS RULE; FEDERAL TAX INFORMATION**

1. This Section applies to the extent Student First Processes Personal Data that constitutes "customer information" under the Safeguards Rule on behalf of a Customer that is a financial institution subject to that Rule (including institutions participating in Title IV federal student aid programs).
2. **Service provider safeguards.** Student First will implement and maintain administrative, technical, and physical safeguards designed to protect the security, confidentiality, and integrity of such Personal Data, consistent with Section 7. On reasonable request, Student First will provide Customer with information regarding Student First's own security controls to support Customer's oversight of service providers under 16 C.F.R. § 314.4(f).
3. **Federal tax information.** Where Personal Data includes federal tax information or return information obtained from the Internal Revenue Service, Student First will: (a)Process FTI solely for the application, award, and administration of financial aid, and not for any other purpose, including product development, analytics, benchmarking, or the training or fitting of any model; (b) not make FTI available to any AI service provider or Process FTI through the AI Functionality, as provided in Section 15.5; (c) limit access to personnel with a need to access FTI for the purposes in clause (a); and (d) impose the requirements of this Section on any Subprocessor that Processes FTI. "**FTI**" means the federal tax information and return information derived from the Internal Revenue Service and contained in the Institutional Student Information Record (ISIR) produced from the FAFSA. FTI does not include financial aid data, award data, student financial or billing information, or other Personal Data that is not IRS-derived return information, even where such data relates to financial aid.
4. **Safeguards for FTI.** Student First will maintain administrative, technical, and physical safeguards for FTI consistent with Section 7, including encryption, logging of access to FTI, and secure disposal. Student First will notify Customer in accordance with Section 10 of any Security Incident involving FTI. Not withstanding Section 10.1, Student First will notify Customer of a Security Incident involving FTI without undue delay and as promptly as reasonably practicable, and in any event sooner than the period in Section 10.1, after Student First becomes aware of the Security Incident, and will provide Customer with the information reasonably necessary for Customer's reporting to the IRS Office of Safe guards and the Treasury Inspector General for Tax Administration. As between the Parties, Customer is responsible for such reporting.

5. **DATA OF MINORS**

1. The Services are designed for and directed to institutions of higher education and are not directed to children. Customer is responsible for determining whether any Data Subject is under the age of 18, or under the age of 13, and for obtaining any consent required under Applicable Data Protection

Law (including COPPA) with respect to such Data Subjects. To the extent Customer, acting as the Data Subject's educational institution, provides or directs the provision of Personal Data of a Data Subject under 13 for use limited to the educational context, Student First will Process that Personal Data solely to provide the Services and will not use it to engage in targeted advertising or to build a profile of the Data Subject for any purpose other than performing the Services. Student First will, on Customer's reasonable request, assist Customer in responding to a parent's or guardian's exercise of rights with respect to such Personal Data.

6. **STUDENT FIRST PROCESSING OBLIGATIONS**

1. **Instructions.** Student First will Process Personal Data only on Customer's documented instructions as described in Section 2.2, including with regard to transfers, unless required to do otherwise by law. Student First will inform Customer if, in its opinion, an instruction infringes Applicable Data Protection Law, provided that Student First has no obligation to monitor Customer's compliance or to provide legal advice.
2. **Confidentiality.** Student First will ensure that personnel authorized to Process Personal Data are bound by appropriate obligations of confidentiality and are informed of the confidential nature of the Personal Data. Access is limited to personnel who need access to perform the Services.
3. **Data minimizationwithin the Services.** Student First will Process only the Personal Data that Customer submits to, or configures the Services to collect within, Student First's environment. Student First does not independently determine what categories of Personal Data are collected or retained; those are determined by Customer's configuration and use of the Services.

7. **SECURITY**

1. **Security program.** Student First maintains additional security documentation, including it independent assessment reports and detailed policies, through its security portal (the "Security Portal"), which is incorporated into this DPA. The measures and documentation in effect as of the effective date of the Agreement govern; Student First may update them from time to time, provided that no update will materially reduce the overall level of protection provided as of the effective date. Student First will make the Security Portal materials available to Customer under Section 13, subject to reasonable confidentiality obligations.
2. **Baseline measures.** Regardless of any change to the Security Portal, Student First will, as a minimum floor: (a) encrypt Personal Data in transit and at rest using industry-standard methods; (b) enforce role-based, least-privilege access controls and multi-factor authentication for administrative and remote access to systems Processing Personal Data; (c) maintain logging and monitoring sufficient to detect and investigate a Security Incident; (d) logically segregate Customer's Personal Data from that of other customers; (e) apply diligence and contractual data protection requirements to Subprocessors consistent with Section 8; (f) maintain backup and recovery measures designed to restore availability of and access to Personal Data following an incident;(g) require personnel authorized to access Personal Data to be bound by confidentiality obligations and to receive periodic security awareness training; and (h) securely delete or destroy Personal Data and media in accordance with Section 17 and industry standards.
3. **Independent assessment.** Student First maintains a SOC 2 Type II assessment of the controls

relevant to the Services, performed by a qualified independent third party. Student First's then-current report, or an executive summary of it, is available to Customer through the Security Portal or on request under Section 13, subject to reasonable confidentiality obligations.

8. **SUBPROCESSORS**

1. **General authorization.** Customer provides general authorization for Student First to engage Subprocessors to Process Personal Data, subject to this Section. Student First's current Subprocessors are listed in Exhibit B (which Student First may maintain at a URL identified in Exhibit B).
2. **Flow-down.** Student First will enter into a written agreement with each Subprocessor that includes data protection obligations that, in substance, are no less protective of Personal Data than those in this DPA to the extent relevant to the nature of the services provided by the Subprocessor. With respect to established infrastructure, hosting, or platform providers that make available standard data protection terms (for example, a published data processing addendum), Student First's acceptance of those standard terms satisfies this Section, provided they afford a materially comparable level of protection. Student First remains responsible for the performance of each Subprocessor's obligations under this DPA.
3. **Notice and objection.** Student First will notify Customer of any intended addition or replacement of a Subprocessor at least thirty (30) days before the new Subprocessor Processes Personal Data, by email or through the Services or the Exhibit B list, at Customer's election. Customer may object on reason able grounds relating to data protection by notice to Student First within that period. The Parties will work in good faith to resolve the objection. Where reasonably feasible, Student First may address the objection by making a commercially reasonable effort to avoid Processing Customer's Personal Data through the objected-to Subprocessor, including by using an alternative Subprocessor or, where applicable, disabling the discrete feature the Subprocessor supports. If the objection cannot be resolved within a reasonable period, Customer may, as its sole and exclusive remedy, terminate the portion of the Services that cannot be provided without the objected-to Subprocessor and receive a pro-rata refund of any prepaid fees for the terminated portion.

9. **CUSTOMER-ENGAGED INTEGRATION AND IMPLEMENTATION VENDORS**

1. **Customer's vendors.** Customer may engage its own integration, implementation, data conversion, or similar service providers (each, a "**Customer Vendor**"), including for services Student First does not provide. Each Customer Vendor is Customer's subprocessor or agent, and not Student First's Subprocessor. Student First is not responsible for any Customer Vendor, for the acts or omissions of any Customer Vendor, or for that Customer Vendor's compliance with Applicable Data Protection Laws.
2. **Access within the Services.** Where Customer grants a Customer Vendor access to Customer's Personal Data within the Services (for example, through credentials Customer issues or authorizes), Customer is responsible for that access, for the credentials and permissions it grants, and for the Customer Vendor's use of the Services and the Personal Data it accesses, including any access from outside the United States. Access by a Customer Vendor within the Services under Customer's authorization does not make the Customer Vendor Student First's Subprocessor.

3. **Export from the Services.** Where Customer or a Customer Vendor exports, downloads, or otherwise removes Personal Data from the Services, Student First's obligations under this DPA do not apply to that exported Personal Data once it is outside the Student First environment, and Customer is responsible for the security and Processing of that Personal Data thereafter.

10. **SECURITY INCIDENT RESPONSE**

    1. **Notification.** Student First will notify Customer of a Security Incident without undue delay and in any event no later than seventy-two (72) hours after Student First becomes aware of the Security Incident. Student First becomes aware of a Security Incident when Student First has a reasonable degree of certainty that a Security Incident, as defined in Section 1, has occurred, which does not include the period during which Student First is investigating an unverified alert or a potential event that does not yet indicate a Security Incident.
    2. **Contents.** To the extent known at the time of notification, Student First will describe the nature of the Security Incident, the categories and approximate number of Data Subjects and records affected, the likely consequences, and the measures taken or proposed to address it and mitigate its effects. Where the required information is not available at the time of initial notification, Student First may provide it in phases without undue further delay as the investigation progresses.
    3. **Investigation and mitigation.** Student First will promptly investigate the Security Incident, take reasonable steps to contain and remediate it, and cooperate with Customer's reasonable requests for information within Student First's possession or control relating to the Security Incident.
    4. **Customer controls external notification.** As between the Parties, Customer is responsible for determining whether, when, and how to notify Data Subjects, regulators, or other third parties of a Security Incident, and for making any such notification. Student First will not notify any Data Subject, regulator, or other third party of a Security Incident on Customer's behalf except at Customer's written direction or where required by law applicable to Student First. Student First will, where reasonably practicable, consult with Customer before making any legally required notification that identifies Customer.
    5. **Costs; no additional liability.** Each Party bears its own costs of complying with this Section. Student First's liability arising from a Security Incident is subject to the limitations of liability in the Agreement. Nothing in this Section requires Student First to provide credit monitoring or similar services except to the extent required by law applicable to Student First, or creates any obligation of Student First to indemnify Customer.
    6. **No admission.** Student First's notification of or response to a Security Incident is not an acknowledgment of fault or liability.

11. **ASSISTANCE WITH DATA SUBJECT RIGHTS**

    1. Taking into account the nature of the Processing, Student First will provide reasonable assistance, by appropriate technical and organizational measures and in so far as possible, to enable Customer to respond to requests from Data Subjects to exercise their rights under Applicable Data Protection Law, including rights of access, correction, deletion, portability, restriction, and objection, and rights relating to automated decision-making.
    2. If Student First receives a request directly from a Data Subject relating to Personal Data, Student

First will, unless legally prohibited, promptly forward the request to Customer and will not respond to the request itself other than to acknowledge receipt and direct the Data Subject to Customer, except at Customer's direction.

3. Customer may use the functionality of the Services to access, correct, delete, and export Personal Data. Where a request cannot be fulfilled through that functionality, Student First will provide reasonable additional assistance at Customer's request.

12. **ASSISTANCE WITH COMPLIANCE OBLIGATIONS**

1. Taking into account the nature of the Processing and the information available to Student First, Student First will provide Customer reasonable assistance with (a) data protection impact assessments and prior consultations with supervisory authorities that Customer is required to carry out under Applicable Data Protection Law, and (b) Customer's obligations to maintain the security of Personal Data and to notify Security Incidents, in each case to the extent relating to Student First's Processing.
2. Student First may make available documentation, such as security summaries, certifications, and completed standardized questionnaires, to facilitate the assistance described in this Section.

13. **RECORDS AND AUDITS**

1. **Information.** Student First will make available to Customer information reasonably necessary to demonstrate compliance with this DPA, which may be satisfied through the Security Portal, Student First's then-current third-party assessment reports(for example, SOC 2), security documentation, and responses to reasonable questionnaires.
2. **Audits.** Where the information described in Section 13.1 is insufficient to demonstrate compliance, and to the extent required by Applicable Data Protection Law, Customer (or a mutually acceptable independent auditor bound by confidentiality) may audit Student First's compliance with this DPA, on at least thirty (30) days' prior written notice, no more than once in any twelve (12)-month period (except as required by a supervisory authority or following a Security Incident affecting Customer's Personal Data), during business hours, subject to Student First's security and confidentiality requirements, and in a manner that does not disrupt Student First's operations or compromise the data of other customers. Each Party bears its own costs of an audit.

14. **DE-IDENTIFIED DATA**

1. **Standard.** Personal Data qualifies as De-Identified Data only if it cannot reasonably be used to infer information about, or otherwise be linked to, a particular Data Subject, and it has been de-identified such that (a) all personally identifiable information has been removed or obscured, including direct and indirect identifiers, such that a student's identity is not personally identifiable, whether through single or multiple releases, taking into account other reasonably available information, consistent with 34 C.F.R. § 99.31(b); and (b) it satisfies the standard for deidentified information under the CCPA and comparable Applicable Data Protection Laws. Student First owns all right, title, and interest in De-Identified Data, subject to this Section.
2. **Commitments.** With respect to De-Identified Data, Student First will (a) take reasonable measures to ensure the information cannot be associated with a Data Subject or household; (b) publicly

commit to maintain and use the information only in de-identified form and not to attempt to re-identify it, except that Student First may attempt re-identification solely to test the effectiveness of its de-identification; and (c) contractually obligate any recipient of the De-Identified Data to comply with the same restrictions and, in turn, to bind its own recipients.

3. **Permitted use.** Subject to Sections 14.1 and 14.2, Student First may use, retain, and disclose De-Identified Data to develop, improve, support, and operate its products and services, including for analytics and bench marking. De-Identified Data is not Personal Data and is not subject to the restrictions on Personal Data in this DPA. Student First will not attempt to re-identify De-Identified Data except as permitted in Section 14.2, and will not combine De-Identified Data with other information in a manner that re-identifies a Data Subject.

15. **ARTIFICIAL INTELLIGENCE**

1. **Scope; no Student First AI.** The Services may include a means ("AI Functionality") through which Customer may connect a third-party AI service that Customer selects, contracts with, and pays for directly ("**Customer's AI Provider**") to Process Personal Data. AI Functionality Processes Personal Data only if and for so longas Customer connects and maintains Customer's AI Provider; if Customer does not do so, the AI Functionality does not Process Personal Data. Student First does not Process, and will not enable the Processing of, Personal Data through any AI model or AI service that Student First itself operates, licenses, or subscribes to, whether directly or indirectly, through any field, feature, underlying service, or endpoint of the Services.
2. **Customer's AI Provider.** Personal Data made available to Customer's AI Provider is Processed by a provider that Customer engages, contracts with, and pays directly, under terms between Customer and that provider. That provider is not Student First's Subprocessor. As between the Parties, Customer is responsible for (a) the terms of its agreement with that provider, including any retention, human review, and training terms; (b) configuring its subscription consistent with Customer's obligations under Applicable Data Protection Laws; and (c) ensuring that provider's Processing complies with Customer's obligations, including under FERPA. Student First makes no representation or warranty regarding Customer's AI Provider or its terms.
3. **Customer responsibility; no advice.** Customer is solely responsible for selecting, contracting with, configuring, and overseeing Customer's AI Provider, including any retention, human review, training, and data residency settings, and for determining whether the AI Functionality is suitable for the categories of Personal Data Customer chooses to Process through it. Any documentation, configuration information, or product materials Student First makes available regarding third-party AI services are provided for informational purposes only, without warranty of any kind, do not constitute legal, regulatory, or compliance advice, and are not a substitute for Customer's own review. Student First has no obligation to monitor, assess, or advise on Customer's configuration of, or compliance of Customer's use of, any AI service.
4. **No training or model fitting by Student First.** Student First will not use Personal Data to train, fine-tune, or otherwise improve any foundation model or any model made available to other customers. Student First does not fit or operate any predictive or machine-learning model on Customer's Personal Data. This Section does not limit Student First's rights with respect to De-Identified Data under Section 14.

5. **Restricted data.** Student First will exclude FTI, Social Security numbers, and parent financial information from the data and database schema made available to Customer's AI Provider, and configures the AI Functionality so that it is designed to prevent the return of those categories of Personal Data. FTI is excluded from the AI Functionality and may not be made available to Customer's AI Provider. Financial aid, award, student account, billing, and payment data, other than FTI, may be made available to Customer's AI Provider through the AI Functionality by default; Customer may select any of those non-FTI categories to exclude, and Student First will configure the AI Functionality to reflect the categories Customer selects.
6. **Human review of outputs.** Outputs of Customer's AI Provider accessed through the AI Functionality, including any risk indicators or predictive scores, are generated by Customer's AI Provider and are decision support only. Customer is responsible for human review of outputs and for any decision concerning a Data Subject. Neither Student First nor the AI Functionality makes, or is intended to make, decisions producing legal or similarly significant effects concerning a Data Subject without human involvement. Student First does not generate, and does not warrant the accuracy, completeness, or fitness for any particular purpose of, any AI-generated output.
7. **Additional AI integration surfaces.** This Section 15 applies to any current or future mechanism by which Student First makes available a means for an AI service, agent, or tool to connect to the Services, including any protocol server (such as a Model Context Protocol server), API, plug-in, or connector, regardless of the name or technology used (each, an "**AI Integration Surface**"). Student First will:

   (a) treat each AI Integration Surface solely as a conduit through which Customer may connect Customer's AI Provider, and not as a means by which Student First itself Processes Personal Data using any AI model or service. Consistent with Section15.1, Student First will not operate, or connect Personal Data to, an AI model or AI service through any AI Integration Surface;

   (b) apply the restrictions in Sections 15.4 (no training) and 15.5 (restricted data) to each AI Integration Surface; and

   (c) where Customer configures Customer's AI Provider to connect to an AI Integration Surface, apply Sections 15.2 and 15.3 (Customer's provider; Customer responsibility) to that configuration.

   This Section does not itself authorize Student First to launch a new AI Integration Surface; any such launch remains subject to Student First's internal AI governance process and, where it constitutes a material change to the Processing described in Exhibit A, to Section 8.3.

16. **PROCESSING LOCATIONS AND INTERNATIONALTRANSFERS**

1. **Primary processing location.** Personal Data is hosted and Processed in the United States, in the cloud environment identified in Exhibit B.
2. **Data subject scope.** The Services are provided to institutions of higher education. Customer represents and covenants that it will not use the Services to submit or Process Personal Data that is subject to the General Data Protection Regulation (EU) 2016/679, the UK GDPR, or any other data

protection law of a jurisdiction outside the United States, unless the Parties have first executed the applicable addendum to this DPA addressing such law. Customer is responsible for determining whether Personal Data it submits is subject to any such law.

3. **Transfer mechanisms.** If and to the extent the Processing falls within the scope of the GDPR, UK GDPR, or an applicable Canadian privacy law, the Parties will cooperate in good faith to put in place an appropriate transfer mechanism and supplementary terms (for example, the European Commission's Standard Contractual Clauses and the UK International Data Transfer Addendum), which upon execution will be incorporated into this DPA and, with respect to Personal Data within their scope, will control in the event of conflict. The Parties do not intend the full apparatus of those instruments to apply to Personal Data outside their scope.
4. **Non-U.S. Data Protection Laws.** If Customer submits Personal Data subject to a data protection law of a jurisdiction outside the United States without the Parties having executed the applicable addendum "International Addendum", (a) Student First's obligations with respect to that Personal Data are limited to those set out in this DPA, and Student First has no liability under such foreign law arising from the absence of the International Addendum; and (b) Customer is responsible for, and will hold Student First harmless from, claims arising from Customer's submission of such Personal Data in breach of Section 16.2.

17. **RETURN AND DELETION OF PERSONAL DATA**

1. **During the term.** Retention of Personal Data during the term of the Agreement is controlled by Customer. Student First retains Personal Data for so long as, and to the extent that, Customer maintains that Personal Data within the Services, and does not independently retain Personal Data beyond what Customer maintains in its instance. Student First does not apply automated retention limits or purge schedules to Customer's Personal Data; Customer is responsible for determining retention periods for each category of Personal Data, including Personal Data of applicants and prospective students who do not enroll, and may use the functionality of the Services to delete Personal Data.
2. **On termination.** Following expiration or termination of the Agreement, Student First will, at Customer's election, return or delete Personal Data in Student First's possession or control within sixty (60) days, except to the extent retention is required by law applicable to Student First. Student First will confirm deletion in writing on Customer's request.
3. **Residual copies; backups.** Personal Data retained in routine backups will be deleted in the ordinary course of Student First's backup rotation, and remains subject to the confidentiality and security obligations of this DPA until deleted. De-Identified Data is not subject to this Section.

18. **LIABILITY**

1. Each Party's liability arising out of or related to this DPA, whether in contract, tort, or under any other theory of liability, is subject to the exclusions and limitations of liability set out in the Agreement. This DPA does not, and is not intended to, expand any Party's liability beyond what the Agreement provides, and does not create any indemnification obligation of Student First.

19. **GENERAL**

1. **Precedence.** This DPA forms part of the Agreement. With respect to the Processing of Personal Data, this DPA controls over the body of the Agreement and any exhibit, schedule, or order form, including any exhibit addressing artificial intelligence functionality, in each case in the event of a conflict. In all other respects the Agreement controls. In case of a conflict between this DPA and an executed transfer mechanism under Section 16, the transfer mechanism controls as to Personal Data within its scope.
2. **Term.** This DPA takes effecton the effective date of the Agreement and continues until Student First has returned or deleted all Personal Data in accordance with Section 17. Provisions that by their nature should survive termination will survive.
3. **Amendment.** This DPA is incorporated into the Agreement, either by execution by both Parties orby reference in the Agreement or an Order Form to the then-current version of this DPA published by Student First at studentfirst.com/dpa. Where incorporated by reference, the version of this DPA in effect as of the effective date of the applicable Agreement or Order Form governs. Student First may also update the published version of this DPA and schedules, on at leasttwenty (20) days' prior written notice to Customer, provided that no update will apply retroactively, and if in good faith Customer reasonably identifies any updated provision which materially diminishes Customer's rights, or Student First's obligations, under applicable laws, Customer and Student First shall use commercially reasonable efforts to refine such provision and in any event such updated provision will not apply to Customer's then-existing Agreement or Order Form until its renewal, unless the Parties agree otherwise in writing. Any other amendment to this DPA requires a written instrument signed by both Parties.
4. **No Professional Advice.** Except for the specific obligations expressly set out in this DPA, Student First is not rendering legal, accounting, or other similar professional services, and makes no claim that Customer's use of the Services will guarantee Customer's compliance with applicable federal or state laws, rules, or regulations. The Services are a tool that Customer uses to support its own compliance; as between the Parties, Customer is responsible for determining what Applicable Data Protection Laws require of Customer and for configuring and using the Services accordingly. Nothing in this Section limits or qualifies Student First's obligations expressly required by Applicable Data Protection Laws. Each institution should seek legal, accounting, and similar professional services from competent providers of its own choosing.
5. **Severability; governing law.** If any provision of this DPA is held invalid or unenforceable, the remainder remains in effect. This DPA is governed by the governing law of the Agreement, except to the extent Applicable Data Protection Law requires otherwise.
6. **Counterparts.** This DPA may be executed in counterparts, including by electronic signature, each of which is an original and all of which together constitute one instrument.

EXHIBIT A
Details of Processing

Item	Detail
Subject matter of Processing	Student First's provision of the Services to Customer under the Agreement.

Item	Detail
Nature and purpose	Hosting, storage, and processing of Personal Data to provide a cloud-based student information system covering admissions and applications, enrollment and registration, academic records, financial aid administration, student finance, advising, and reporting, together with the AI Functionality described in Section 15.
Duration	The term of the Agreement, plus the deletion period in Section 17. Retention during the term is determined by Customer; Student First does not apply automated purge schedules.
Frequency	Continuous, for the duration of the Agreement.
Categories of Data Subjects	Applicants and prospective students, including those who do not enroll; enrolled students; withdrawn and former students; alumni; parents and guardians (including in connection with financial aid); Customer personnel (faculty, staff, and administrators) who use the Services.
Categories of Personal Data	Identifiers and contact data; demographic data; application and admissions data; academic and enrollment records; financial aid data, including FAFSA/ISIR data and Title IV records; federal tax information derived from IRS data (stored on the ISIR; excluded from the AI Functionality per Sections 4.3 and 15.5); Social Security numbers; parent financial information; student account and billing data; advising and student success data, including risk indicators generated by the AI Functionality; user account and authentication data for Customer personnel.
Sensitive / special-category data	Social Security numbers, financial account and federal tax information, health, disability and accommodation, immigration and visa status, criminal history, and racial and ethnic data.
Processing locations	United States.
Subprocessors	As set out in Exhibit B.

EXHIBIT B
Subprocessors

Student First's current Subprocessors are listed below. Student First may maintain an up-to-date list at studentfirst.com/legal/subprocessors, which is incorporatedby reference.

Subprocessor	Service Provided	Data Categories	Processing Location
Microsoft Corporation (Azure)	Cloud infrastructure hosting — compute, storage, database (Azure SQL), networking, AKS	All customer/student data processed by the platform (full dataset)	United States (default); European Economic Area for customers with EU data residency requirements
Google LLC (reCAPTCHA)	Bot/fraud protection on public-facing forms (login, registration)	IP address, device/browser fingerprint, interaction telemetry	Google global infrastructure
Zendesk	Customer support / ticketing platform	Ticket content, support correspondence, end-user contact details, and any personal data submitted via free-text fields	United States

SCHEDULE 1
Jurisdiction-Specific Requirements

This Schedule sets out obligations that are specific to a particular Applicable Data Protection Law and are not capable of harmonization into a single standard under Section 2.4. Each item applies only to Personal Data within the scope ofthe identified law.

Law / Jurisdiction	Requirement	Applies to
CCPA (California)	Service provider terms in Section 2.3 apply; Student First will assist Customer with consumer requests under Section 11;	Personal information of California residents not exempt under the FERPA data-level exemption (e.g., applicant/prospect data of for-profit-institution customers).
FERPA (federal)	School official terms in Section 3.	Education Records of FERPA-covered institutions.
Safeguards Rule (federal)	Sections 4.1–4.2.	“Customer information” of Title IV / financial-institution customers.
IRC § 6103 / HEA § 483; IRS Pub. 1075 (federal)	Sections 4.3–4.4: use limited to aid administration; no access from outside the United States; flow-down to Subprocessors.	Federal tax information obtained through the FAFSA data exchange.
GDPR / UK / Canada	Transfer mechanism and supplementary terms under Section 16, if triggered.	Personal Data within scope of those laws, if any.