STUDENT DATA PRIVACY AGREEMENT

Data Processing Agreement (DPA)

Based on NDPA Standard Version 2.2 Framework

School District / Local Education Agency

New York State Network for Youth Success, Inc.

And

TransAct Communications LLC dba Pathwise

Version 1.0 — Based on NDPA Standard v2.2

TransAct Communications LLC dba Pathwise
19217 36th Ave W, Suite 213, Lynnwood, WA 98036
425.977.2100 | privacy@pathwisek12.com | www.pathwisek12.com

STUDENT DATA PRIVACY AGREEMENT

This Student Data Privacy Agreement ("DPA") is entered into on the date of full execution (the "Effective Date") and is entered into by and between:

LEA (Local Education Agency)	Provider
New York State Network for Youth Success, Inc.	TransAct Communications LLC dba Pathwise
415 River Street, 2nd Floor Troy, NY 12180	19217 36th Ave W, Suite 213 Lynnwood, WA 98036

PREAMBLE

WHEREAS, the Provider is providing educational or digital Services, as defined in Exhibit "A" (the "Services"), to LEA, which Services may include: (a) cloud-based Services for the digital storage, management, and retrieval of Student Data; and/or (b) digital educational software that authorizes Provider to access, store, and use Student Data; and

WHEREAS, the Provider and LEA have entered into a Service Agreement (as defined herein), to provide certain Services to the LEA as set forth in the Service Agreement, and this DPA (collectively the "Agreement"),

WHEREAS, the Provider and LEA recognize the need to protect Student Data and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. 1232g (34 C.F.R. Part 99); the Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h; and the Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6506 (16 C.F.R. Part 312),

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

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

General Offer of Privacy Terms.

The Provider has signed Exhibit "E" to the Standard Clauses, otherwise known as "General Offer of Privacy Terms" enabling other LEAs to enter into the same terms of this DPA with Provider.

Special Provisions. (Check if Required)

☑ If checked, the Supplemental State Terms attached hereto as Exhibit "G" are hereby incorporated by reference into this DPA in their entirety.

If the Parties desire to change any terms, use the 'Vendor-Specific' Agreement or 'District-Modified' Agreement.

DESIGNATED REPRESENTATIVES AND EXECUTION

The designated representative for the LEA for this DPA is:

Alli Lidie	CEO
415 River Street, 2nd Floor, Troy, NY 12180	
518-694-0660, ext 2	alli@networkforyouthsuccess.org

The designated representative for the Provider for this DPA is:

Todd Yates, PhD	CISO
19217 36th Ave W, Suite 213 Lynnwood, WA 98036	
425-977-2100	todd.yates@pathwisek12.com

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

LEA	PROVIDER:
New York State Network for Youth Success, Inc.	TransAct Communications LLC dba Pathwise
	Todd Yates, PhD
Alli Lidie, CEO	Todd Yates, PhD, CISO

Each Party is responsible to promptly notify the other Party of changes to the notice information.

Notices to Provider	Notices to LEA
TransAct Communications LLC Custodian 19217 36th Ave W, Suite 213 Lynnwood, WA 98036 privacy@transact.com	New York State Network for Youth Success, Inc. CEO 415 River Street, 2nd Floor, Troy, NY 12180 alli@networkforyouthsuccess.org

Security Notices to Provider (Required per Section 5.3)	Security Notices to LEA (Required per Section 5.3)
Todd Yates, PhD CISO 19217 36th Ave W, Suite 213 Lynnwood, WA 98036 security@transact.com	Alli Lidie CEO 415 River Street 2nd Floor Troy, NY 12180 alli@networkforyouthsuccess.org

STANDARD CLAUSES

ARTICLE I: PURPOSE AND SCOPE

1.1 Purpose of DPA.

The purpose of this DPA is to describe the duties and responsibilities to protect Student Data including compliance with all applicable federal and state privacy laws, rules, and regulations, all as may be amended from time to time. In performing the Services, the Provider shall be considered a School Official with a legitimate educational interest, and performing Services otherwise provided by the LEA. With respect to its use and maintenance of Student Data, Provider shall be under the direct control and supervision of the LEA as set forth in this DPA and the Service Agreement.

1.2 Description of Products and Services.

A description of all products and services covered by the Agreement, and information specific to this DPA, are listed in Exhibit "A". If Provider needs to update any information on Exhibit "A" (such as updating with new provided services), they may do so by completing an Addendum and sending a copy to the LEA.

Provider may add or delete products or services subject to this DPA under the following circumstances:

1. **Deleted products or services:** The products or services have been discontinued and are no longer available from the Provider.
2. **Added products or services:** The added products or services are either:
    a. a direct replacement, or substantially equivalent to the original products or services listed in the DPA, or
    b. the added products or services result in new or enhanced capabilities, new modules, technology advancements, and/or service categories relating to the listed products or services that Provider did not have at the time the DPA was signed.

If an added product or service requires additional Data Elements, Provider must update Exhibit "B". The Provider must notify the LEA of the existence and contents of any Addendum. The LEA will have thirty (30) days from receipt to object in writing. If no written objection is received, it will become incorporated into the DPA.

1.3 Student Data to Be Provided.

In order to perform the services, the Provider shall process Student Data as identified by the Provider in the Schedule of Data, attached hereto as Exhibit "B". Student Data may be provided by the LEA or created by students. If Provider needs to update any information on Exhibit "B", they may do so via Addendum and sending a copy to the LEA. Provider must add data elements to Exhibit "B" when a material change has occurred. The Provider must notify the LEA of the existence and contents of an Addendum modifying Exhibit "B". The LEA will have thirty (30) days from receipt to object. If no written objection is received it will become incorporated into the DPA.

1.4 DPA Definitions.

Capitalized terms used in this DPA shall have the meanings set forth in Exhibit "C". With respect to the treatment of Student Data, in the event of a conflict, definitions used in this DPA shall prevail over terms used in any other writing, including, but not limited to, the Service Agreement.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

2.1 Student Data Property of LEA.

As between LEA and Provider, all Student Data processed by the Provider, or created by students, pursuant to the Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data processed by the Provider, including any modifications or additions or any portion thereof from any source, are also subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement, shall remain the exclusive property of the LEA.

2.2 Parent, Legal Guardian, and Student Access.

The LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student (as defined in FERPA) may review Student Data and request deletion or modification, and request delivery of a copy of the Student Data. In support of this, the Provider shall establish reasonable procedures by which the LEA may access, and correct, if necessary, Education Records and/or Student Data, and make a copy of the data available to the LEA or (at the LEA's direction) to the parent, legal guardian, or eligible student directly. If the LEA is not able to review or update the Student Data itself, Provider shall respond no later than thirty (30) days from the date of the request or pursuant to the time frame required under state law, whichever is sooner.

In the event that a parent or legal guardian of a student or eligible student contacts the Provider to correct, delete, review, or request delivery of a copy of any Student Data, the Provider shall refer that person to the LEA, who will follow the necessary and proper procedures regarding the requested information.

2.2.1 This DPA does not impede the ability of students to download, export, or otherwise save or maintain their own Student Generated Content directly from Provider. Nor does it impede the ability of Providers to offer LEAs features to allow such ability.

2.2.2 In the event that Student Generated Content is transferred to the control of the student, parent, or legal guardian, the copy of such Student Generated Content that is in the control of such person is no longer considered Student Data.

2.3 Subprocessors.

Provider shall enter into a Subprocessor Agreement with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA. Every Subprocessor Agreement must provide that the Subprocessor will not sell the Student Data.

ARTICLE III: DUTIES OF LEA

3.1 Provide Data in Compliance with Applicable Laws.

LEA shall use the Services and provide Student Data in compliance with all applicable federal and state privacy laws, rules, and regulations, all as may be amended from time to time.

3.2 Annual Notification of Rights.

If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), LEA shall include a specification of criteria for determining who constitutes a School Official and what constitutes a legitimate educational interest in its annual notification of rights.

3.3 Reasonable Precautions.

LEA shall employ administrative, physical, and technical safeguards designed to protect usernames, passwords, and any other means of gaining access to the Services and/or hosted Student Data from unauthorized access, disclosure, or acquisition by an unauthorized person.

3.4 Unauthorized Access Notification and Assistance.

LEA shall notify Provider within seventy-two (72) hours of any confirmed Data Breach to the Services, LEA's account, or any Student Data that poses a privacy or security risk. If requested by Provider, LEA will provide reasonable assistance to Provider in any efforts by Provider to investigate and respond to such Data Breach.

ARTICLE IV: DUTIES OF PROVIDER

4.1 Privacy and Security Compliance.

The Provider shall comply with all laws and regulations applicable to Provider's protection of Student Data privacy and security, and at the direction of the LEA shall cooperate with any state or federal government-initiated audit of the LEA's use of the Services.

4.2 Authorized Use.

The Student Data processed pursuant to the Services shall be used by the Provider for no purpose other than performing the Services outlined in Exhibit "A", or as instructed by the LEA.

4.3 Provider Employee Obligation.

Provider shall require all of Provider's employees who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Student Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee with access to Student Data pursuant to the Service Agreement.

4.4 No Disclosure.

Provider acknowledges and agrees that it shall not sell or disclose any Student Data or any portion thereof, including without limitation, user content or other non-public information and/or Personally Identifiable Information contained in the Student Data.

4.4.1 Exceptions to No Disclosure.

4.4.1.1 This prohibition against disclosure will not apply to Student Data where disclosure is directed or permitted by the LEA or this DPA.

4.4.1.2 The provision to not sell Student Data shall not apply to a Change of Control.

4.4.1.3 This prohibition against disclosure shall not apply to Student Data disclosed pursuant to a judicial order or lawfully issued subpoena or warrant.

4.4.1.4 This prohibition against disclosure shall not apply to Student Data disclosed to Subprocessors performing Services on behalf of the Provider pursuant to this DPA.

4.4.1.5 Should law enforcement or other government entities ("Requesting Party(ies)") provide a judicial order or lawfully issued subpoena or warrant to the Provider with a request for Student Data, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party.

4.4.1.6 Notification under 4.4.1.5 is not required if the judicial order or lawfully issued subpoena or warrant states not to inform the LEA of the request.

4.4.1.7 Should the LEA be presented with a judicial order or lawfully issued subpoena to disclose Student Generated Content or other Student Data, the Provider shall cooperate with the LEA in delivering such data.

4.4.1.8 This prohibition against disclosure shall not apply to LEA-authorized users of the Services, which may include parents and legal guardians.

4.4.1.9 This prohibition against disclosure shall not apply to protect the safety of users or others, if and only if, an LEA employee who has specifically been authorized to declare a health or safety emergency has done so and all requirements under 34 CFR §§ 99.31(a)(10) and 99.36 have been fulfilled by the LEA.

4.4.1.10 This prohibition against disclosure shall not apply to protect the integrity or security of the Service, where such disclosure is made to a Subprocessor engaged for the specific purpose of investigating a potential Data Breach as set forth in 5.4.

4.5 De-Identified Data.

Provider agrees not to attempt to re-identify De-Identified Data without the written direction of the LEA. De-Identified Student Data may be used by the Provider for those purposes allowed under applicable laws, as well as: (1) assisting the LEA or other governmental agencies in conducting research and other studies; (2) research, development, and improvement of the Provider's educational sites, Services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or dispose of Student Data. Except for Subprocessors, Provider agrees not to transfer De-Identified Data to any third party unless the transfer is expressly directed or permitted by the LEA or this DPA. If Provider chooses to create De-Identified Data, its process must comply with either NIST de-identification standards or US Department of Education guidance on de-identification.

4.6 Disposition of Student Data.

Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. If the Provider has a standard retention and destruction schedule, that schedule shall apply to Student Data as long as this DPA is active. At the termination of this DPA, the Provider shall, unless directed otherwise by the LEA, dispose of, or delete Student Data obtained by the Provider under the Agreement within sixty (60) days of termination (unless otherwise required by law). The LEA may provide the Provider with special instructions for the disposition of Student Data by transmitting to Provider Exhibit "D", attached hereto.

4.7 Advertising Limits.

Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; (b) develop a profile of a student, family member/guardian, or group, for any purpose other than providing the Service to LEA; or (c) for any commercial purpose other than to provide the Service to the LEA, or as authorized by the LEA or the parent/guardian. Targeted Advertising is strictly prohibited. However, this section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); (ii) to make product recommendations to account holders that are not considered Targeted Advertising; or (iii) to notify account holders about new education product updates, features, or Services.

ARTICLE V: DATA SECURITY AND BREACH PROVISIONS

5.1 Data Storage.

If Student Data is stored outside the United States, Provider will provide a list of countries where data is stored, in Exhibit "B".

5.2 Security Audits.

Provider will conduct a security audit or assessment no less than once per year, and upon a Data Breach. Upon 10 days' notice and execution of confidentiality agreement, Provider will provide the LEA with a copy of the audit report, subject to reasonable and appropriate redaction.

5.3 Data Security.

The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security of Student Data. The Provider shall implement an adequate Cybersecurity Framework that incorporates one or more of the nationally or internationally recognized standards set forth in Exhibit "F". Provider shall provide, in the Preamble to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.

5.4 Data Breach.

In the event that Provider confirms a Data Breach, the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the Data Breach, unless notification within these time limits would disrupt investigation of the Data Breach by law enforcement. Provider shall follow the following process:

(1) The Data Breach notification shall include, at a minimum: (a) name and contact information of the Provider; (b) the date of the notice; (c) the date of the Data Breach or date range; (d) whether the notification was delayed due to a law enforcement investigation; (e) a general description of the Data Breach; (f) a description of the Student Data reasonably believed to have been the subject of the Data Breach; and (g) identification of impacted individuals.

(2) Provider agrees to adhere to all applicable federal and state laws with respect to a Data Breach related to the Student Data, including any required responsibilities and procedures for notification and mitigation of any such Data Breach.

(3) Provider further acknowledges and agrees to have a written Data Breach response plan that is consistent with applicable industry standards and federal and state law for responding to a Data Breach, and agrees to provide LEA, upon reasonable written request, with a summary of said written Data Breach response plan.

(4) LEA shall provide notice and facts surrounding the Data Breach to the affected students, parents, or guardians.

(5) In the event of a Data Breach originating from LEA's use of the Service or otherwise a result of LEA's actions or inactions, Provider shall reasonably cooperate with LEA to the extent necessary to expeditiously secure Student Data and may request costs incurred as a result of such Data Breach.

CONTRACT TERMS

Term and Termination. In the event that either Party seeks to terminate this DPA, they may do so by written notice if the Service Agreement has lapsed or has been terminated. Either party may terminate this DPA and any Service Agreement or contract if the other party breaches any terms of this DPA. This DPA shall stay in effect for as long as the Provider retains the Student Data, as set forth in Article IV, Section 4.6. In the case of a Change of Control, the LEA has

the authority to terminate the DPA if it reasonably believes that the successor cannot uphold the terms and conditions herein or having a contract with the successor would violate the LEA's policies or state or federal law.

Data Disposition on Service Agreement Termination. If the Service Agreement is terminated, the Provider shall dispose of all of LEA's Student Data pursuant to Article IV, Section 4.6 of the Standard Clauses.

Notices. All notices or other communication required or permitted to be given hereunder must be made in writing and may be given via e-mail transmission, first-class mail, or a mutually agreed upon method sent to the designated representatives documented in the Preamble.

Priority of Agreements. This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. With respect to the treatment of Student Data only, in the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

Entire Agreement. This DPA and the Service Agreement constitute the entire agreement of the Parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the Parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived only with the signed written consent of both Parties.

Severability. Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction.

Governing Law, Venue, and Jurisdiction. This DPA will be governed by and construed in accordance with the laws of the state of the LEA, without regard to conflicts of law principles. Each party consents and submits to the sole and exclusive jurisdiction to the state and federal courts for the county of the LEA for any dispute arising out of or relating to this DPA or the transactions contemplated hereby.

Successors Bound. This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a Change of Control. In the event of a Change of Control, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of such Change of Control. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement.

Authority. Each signatory confirms they are authorized to bind their institution to this DPA in its entirety.

Waiver. No delay or omission by either party to exercise any right hereunder shall be construed as a waiver of any such right and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

EXHIBIT A: PRODUCTS AND SERVICES

This DPA covers access to and use of **TransAct Communications LLC dba Pathwise**'s existing Services described below that collect, process, or transmit Student Data, as identified below:

Product / Service Name	Description	URL / Access Point
All products by Pathwise	All SaaS services for Pathwise	

Service Agreement Reference:

Subcontract for the New York State School-Age Technical Assistance Resource Center (SATARC) under NYS OCFS Contract C030890

Additional Service Notes:

Any additional notes regarding the Services

EXHIBIT B: SCHEDULE OF STUDENT DATA

All data elements identified in this Exhibit are correct at time of signature. For each data element, indicate if it is Required (R) or Optional (O) for the product(s) listed. Add product names in the column headers.

Category of Data / Data Elements	[Product 1]	[Product 2]	[Product 3]
Application Technology Metadata			
IP Addresses of users, use of cookies, etc.	X		
Other application technology metadata	X		
Application Use Statistics			
Metadata on user interaction with application	X		
Assessment			
Standardized test scores			
Observation data			
Voice recordings			
Other assessment data			
Attendance			
Student school (daily) attendance data	X		
Student class attendance data			
Communication			
Online communication captured (emails, blog entries)	X		
Conduct			
Conduct or behavioral data			
Demographics			
Date of birth	X		
Place of birth			
Gender	X		
Ethnicity or race	X		
Language information (native or primary language)			
Other demographic information			
Enrollment			
Student school enrollment			
Student grade level	X		
Homeroom			
Guidance counselor			
Specific curriculum programs			
Year of graduation			
Other enrollment information			
Parent/Guardian Contact Information			
Address	X		
Email	X		
Phone	X		

Category of Data / Data Elements	[Product 1]	[Product 2]	[Product 3]
Parent/Guardian ID			
Parent ID number (created to link parents to students)	X		
Parent/Guardian Name			
First and/or last	X		
Schedule			
Student scheduled courses			
Teacher names			
Special Indicator			
English language learner information			
Low-income status			
Medical alerts/health data			
Student disability information	X		
Specialized education Services (IEP or 504)	X		
Living situations (homeless/foster care)	X		
Other indicator information			
Student Contact Information			
Address	X		
Email	X		
Phone	X		
Student Identifiers			
Local (school district) ID number	X		
State ID number	X		
Provider/app assigned student ID number	X		
Student app username	X		
Student app passwords	X		
Student Name			
First and/or last	X		
Student In App Performance			
Program/application performance			
Student Program Membership			
Academic or extracurricular activities			
Student Survey Responses			
Student responses to surveys or questionnaires			
Student Work			
Student Generated Content (writing, pictures, etc.)			
Other student work data			
Transcript			
Student course grades			
Student course data			
Student course grades/performance scores			
Other transcript data			

Category of Data / Data Elements	[Product 1]	[Product 2]	[Product 3]
Transportation			
Student bus assignment	X		
Student pick up and/or drop off location	X		
Student bus card ID number	X		
Other transportation data	X		
Other			
Other data collected (specify below)			
None			
No Student Data collected at this time			

If Student Data is stored outside the United States, Provider shall list below the countries where data is stored:

'N/A — all data stored in the United States

EXHIBIT C: DEFINITIONS

Change of Control: Any merger, acquisition, consolidation, or other business reorganization or sale of all or substantially all of the assets of Provider or of the portion of Provider that performs the Services in the Service Agreement.

Contextual Advertising: Contextual advertising is the delivery of advertisements based upon a current visit to a website or a single search query, without the collection and retention of data about the consumer's online activities over time.

Data Breach: An unauthorized release, access to, disclosure, or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider in violation of applicable state or federal law.

De-Identified Data: Records and information are considered to be De-Identified Data when all Personally Identifiable Information has been removed or obscured, such that the remaining information does not reasonably identify a specific student, including, but not limited to, any information that, alone or in combination is linkable to a specific student.

Education Records: Education Records shall have the meaning set forth under FERPA 20 U.S.C. 1232 g(a)(4) and 34 CFR § 99.3.

LEA: For the purpose of this DPA, the LEA is the educational entity that is a Party to this Agreement. An LEA can be a state agency, an educational service agency, a charter school, school system, or a private school or school system, in addition to the federal definition of Local Education Agency (LEA).

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

Personally Identifiable Information: Means Personally Identifiable Information or PII as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law.

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

Service Agreement: Refers to the quote, corresponding contract, purchase order, terms of service, and/or terms of use.

Student Data: Student Data includes any data, whether gathered, created, or inferred by Provider or provided by LEA or its users, students, or students' parents/guardians, for a school purpose, that is descriptive of the student including, but not limited to, information in the student's Education Record, persistent unique identifiers, or any other information or identification number that would provide information about a specific student. Student Data includes Metadata that has not been stripped of all direct and indirect identifiers. Student Data further includes Personally Identifiable Information (PII). Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local laws and regulations. Student Data shall not include properly De-Identified Data or anonymous usage data regarding a student's or LEA's use of Provider's Services.

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

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

Subprocessor Agreement: An agreement between Provider and a third party Subprocessor. A Subprocessor Agreement includes either a written agreement or an acceptance of terms and conditions (e.g., click through agreements).

Targeted Advertising: Targeted Advertising means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the Provider Internet website, online service, or mobile application by such student or the retention of such student's online activities or requests over time for the purpose of targeting subsequent advertisements. Targeted Advertising does not include Contextual Advertising.

EXHIBIT D: SPECIAL INSTRUCTIONS FOR DISPOSITION OF STUDENT DATA

After this DPA takes effect, if the LEA has special requirements for the disposition of Student Data that are not expressed in Section 4.6, the LEA may fill in this form and deliver it to the Provider.

The Provider and the LEA must not fill in this form at the initiation of the DPA.

Insert Name of District or LEA

("LEA") instructs Provider to dispose of Student Data obtained by Provider pursuant to the terms of the DPA between LEA and Provider. The terms of the disposition are set forth below:

1. Extent of Disposition

☐ Disposition is partial. The scope of Student Data to be disposed of is set forth below or found in an attachment to this form:

Insert categories of Student Data here

☐ Disposition is complete. Disposition extends to all Student Data.

2. Nature of Disposition

☐ Disposition shall be by destruction or deletion of Student Data.

☐ Disposition shall be by a transfer of Student Data. The Student Data shall be transferred to the following site as follows:

Insert or attach special instructions

3. Timing of Disposition

☐ As soon as commercially practicable

☐ On Provider's standard destruction schedule

☐ By [Insert Date]

4. De-Identified Data

☐ The Provider certifies that they have de-identified the Student Data, as defined elsewhere in this Agreement, and disposed of all copies of Student Data that were not de-identified in accordance with this Schedule and the DPA. As of [Insert Date]

5. Other:

Other special instructions or notes

Authorized Representative of LEA Date	Authorized Representative of Provider Date

EXHIBIT E: GENERAL OFFER OF PRIVACY TERMS

By signing below, **TransAct Communications LLC dba Pathwise** ("Provider") makes a general offer of the privacy terms set forth in this DPA to any LEA that desires to subscribe to the Provider's Services. Any LEA that executes this Exhibit "E" shall be considered a "Subscribing LEA" and shall be entitled to the same privacy protections set forth in this DPA.

Provider Confirmation:

The Provider confirms that it has reviewed this DPA in its entirety and agrees to be bound by the terms of this DPA with any Subscribing LEA.

PROVIDER:

TransAct Communications, LLC dba Pathwise	
19217 36th Avenue W, Suite 213, Lynnwood, WA 98036	
Todd Yates, PhD	CISO
todd.yates@pathwisek12.com	425-977-2100
Todd Yates, PhD	07/24/2026
Signature	Date

Subscribing LEA Instructions: To subscribe to this DPA, the LEA completes the information below and returns to Provider.

Network for Youth Success	
415 River Street, 2nd Floor, Troy, NY 12180	
Alli Lidie	CEO
alli@networkforyouthsuccess.org	518-694-0660, ext 2
Alli Lidie	7/24/26
Signature	Date

EXHIBIT F: ADEQUATE CYBERSECURITY FRAMEWORKS

Provider must mark one or more frameworks with which it complies. The Provider may change which framework it complies with without invalidating or changing the DPA, but must notify the LEA of such change in accordance with the notification requirements of the DPA.

FRAMEWORK(S) — Check all that apply
☐ Global Education Security Standard - https://sdpc.a4l.org/gess/
☐ NIST Cybersecurity Framework (CSF)
☑ NIST SP 800-53 Security and Privacy Controls for Information systems and organizations
☐ NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
☑ ISO 27000 series, Standards for implementing organization security and management practices
☐ CIS Center for Internet Security Critical Security Controls
☐ Cybersecurity Maturity Model Certification (CMMC, ~FAR/DFAR)
☐ Other (specify):

Optional security programs and measures (Section 5.3):

Optional security program detail

EXHIBIT G: SUPPLEMENTAL STATE TERMS FOR NEW YORK

This Exhibit is an optional set of supplemental terms designed to address state-specific data privacy statute requirements. Use only if this Exhibit is needed to meet the requirements of the LEA's state laws. The scope of these State Supplements is to cite and address any state-specific data privacy statutes and their requirements to the extent that they require terms in addition to or different from the Standard Clauses.

State:

New York

Applicable State Statute(s):

State Name and Citation (e.g., NY Education Law § 2-d, SOPIPA, etc.)

Supplemental Terms (list any additional or modified obligations required by state law):

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

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

8. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."

9. To amend Article IV, Section 3 to add: Provider shall ensure that all its employees and subprocessors who have Access to or will receive Student Data and APPR Data will be trained on the federal and state laws governing confidentiality of such Student Data and APPR Data prior to receipt. Access to or Disclosure of Student Data and APPR Data shall only be provided to Provider's employees and subprocessors who need to know the Student Data and APPR Data to provide the services and such Access and/or Disclosure of Student Data and APPR Data shall be limited to the extent necessary to provide such services.

10. To replace Article IV, Section 6 (Disposition of Data) with the following: Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within ninety (90) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Provider is prohibited from retaining disclosed Student Data or continuing to Access Student Data beyond the term of the Service Agreement unless such retention is expressly authorized for a prescribed period by the Service Agreement, necessary for purposes of facilitating the transfer of disclosed Student Data to the LEA, or expressly required by law. The confidentiality and data security obligations of Provider under this DPA shall survive any termination of this contract to which this DPA is attached but shall terminate upon Provider's certifying that it and it's subprocessors, as applicable: (a) no longer have the ability to Access any Student Data provided to Provider pursuant to the Service Agreement and/or (b) have destroyed all Student Data and APPR Data provided to Provider pursuant to this DPA. The Provider agrees that the timelines for disposition of data will be modified by any assurance of discontinuation, which will control in the case of a conflict. Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all student data after providing the LEA with ninety (90) days prior notice. The duty to dispose of student data shall not extend to Student Data that had been deidentified or placed in a separate student account pursuant to section II 3. The LEA may employ a "Directive for Disposition of Data" form, a copy of which is attached hereto as Exhibit "D", or, with reasonable notice to the Provider, other form of its choosing. No further written request or notice is required on the part of either party prior to the disposition of Student Data described in "Exhibit D".

11. To amend Article IV, Section 7 to add: 'Notwithstanding the foregoing, Provider is prohibited from using Student Data or APPR data for any Commercial or Marketing Purpose as defined herein. And add after (iii) account holder, "which term shall not include students."

12. To replace Article V, Section 1 (Data Storage) to state: Student Data and APPR Data shall be stored within the United States and Canada only. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.

13. To replace Article V, Section 2 (Audits) to state: No more than once a year or following an unauthorized Access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA or its designee(s) to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA . The Provider will cooperate reasonably with the LEA or its designee(s) and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable Access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA.

Upon request by the New York State Education Department's Chief Privacy Officer (NYSED CPO), Provider shall provide the NYSED CPO with copies of its policies and related procedures that pertain to the protection of information. In addition, the NYSED CPO may require Provider to undergo an audit of its privacy and security safeguards, measures, and controls as they pertain to alignment with the requirements of New York

State laws and regulations, and alignment with the NIST Cybersecurity Framework. Any audit required by the NYSED CPO must be performed by an independent third party at Provider's expense and the audit report must be provided to the NYSED CPO. In lieu of being subject to a required audit, Provider may provide the NYSED CPO with an industry standard independent audit report of Provider's privacy and security practices that was issued no more than twelve months before the date that the NYSED CPO informed Provider that it required Provider to undergo an audit. Failure to reasonably cooperate with any of the requirements in this provision shall be deemed a material breach of the DPA.

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

14. To replace Article V. Section 4 (Data Breach) to state: In the event of a Breach as defined in 8 NYCRR Part 121.1 Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:
    a. The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:
        i. The name and contact information of the reporting LEA subject to this section.
        ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
        iii. If the information is possible to determine at the time the notice is provided, then either the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
        iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided; and
        v. The number of records affected, if known; and
        vi. A description of the investigation undertaken so far; and
        vii. The name of a point of contact for Provider.
    b. Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
    c. Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a summary of said written incident response plan.
    d. LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians. Where a Breach of Student Data and/or APPR Data occurs that is attributable to Provider and/or its Subprocessors, Provider shall pay for or promptly reimburse LEA for the full cost of notification to Parents, Eligible Students, teachers, and/or principals.
    e. In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.
    f. Provider and its subprocessors will cooperate with the LEA, the NYSED Chief Privacy Officer and law enforcement where necessary, in any investigations into a Breach. Any costs incidental to the required cooperation or participation of the Provider will be the sole responsibility of the Provider if such Breach is attributable to Provider or its subprocessors.

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

a. "Subprocessor" is equivalent to subcontractor. It is a third party who the provider uses for data collection, analytics, storage, or other service to allow Provider to operate and/or improve its service, and who has access to Student Data.

b. "Provider" is also known as third party contractor. It any person or entity, other than an educational agency, that receives student data or teacher or principal data from an educational agency pursuant to a contract or other written agreement for purposes of providing services to such educational agency, including but not limited to data management or storage services, conducting studies for or on behalf of such educational agency, or audit or evaluation of publicly funded programs. Such term shall include an educational partnership organization that receives student and/or teacher or principal data from a school district to carry out its responsibilities and is not an educational agency and a not-for-profit corporation or other non-profit organization, other than an educational agency.

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

EXHIBIT H: LEA Documents

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

- https://www.transact.com/privacy-policy
- https://www.transact.com/terms-of-use

This DPA template was prepared by TransAct Communications LLC dba Pathwise based on the NDPA Standard Version 2.2 framework. This document is a template and does not constitute legal advice. Parties are encouraged to have this agreement reviewed by legal counsel prior to execution.