Pathful Connect

Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

EDUTECH

CONTRACT ADDENDUM

Protection of Student Personally Identifiable Information

1. Applicability of This Addendum

The Wayne-Finger Lakes BOCES/EduTech) and Pathful, Ir **("Vendor")** are parties to a contract dated 4/19/23 ("the underlying contract") governing the terms under which BOCES accesses, and Vendor provides, Pathful Conne ("Product"). Wayne-Finger Lakes BOCES/EduTech use of the Product results in Vendor receiving student personally identifiable information as defined in New York Education Law Section 2-d and this Addendum. The terms of this Addendum shall amend and modify the underlying contract and shall have precedence over terms set forth in the underlying contract and any online Terms of Use or Service published by Vendor.

2. Definitions

2.1. "Protected Information", as applied to student data, means "personally identifiable information" as defined in 34 CFR Section 99.3 implementing the Family Educational Rights and Privacy Act (FERPA) where that information is received by Vendor from BOCES or is created by the Vendor's product or service in the course of being used by BOCES.

2.2. "Vendor" means {Pathful, Inc. .

2.3. "Educational Agency" means a school BOCES, board of cooperative educational services, school, or the New York State Education Department; and for purposes of this Contract specifically includes Wayne-Finger Lakes BOCES/EduTech.

2.4. "BOCES" means the Wayne-Finger Lakes BOCES/EduTech.

2.5. "Parent" means a parent, legal guardian, or person in parental relation to a Student.

2.6. "Student" means any person attending or seeking to enroll in an educational agency.

2.7. "Eligible Student" means a student eighteen years or older.

2.8. "Assignee" and "Subcontractor" shall each mean any person or entity that receives, stores, or processes Protected Information covered by this Contract from Vendor for the purpose of enabling or assisting Vendor to deliver the product or services covered by this Contract.

2.9. "This Contract" means the underlying contract as modified by this Addendum.

3. Vendor Status

Vendor acknowledges that for purposes of New York State Education Law Section 2-d it is a third-party contractor, and that for purposes of any Protected Information that constitutes education records under the Family Educational Rights and Privacy Act (FERPA) it is a school official with a legitimate educational interest in the educational records.

4. Confidentiality of Protected Information

Vendor agrees that the confidentiality of Protected Information that it receives, processes, or stores will be handled in accordance with all state and federal laws that protect the confidentiality of Protected Information, and in accordance with the BOCES Policy on Data Security and Privacy, a copy of which is Attachment B to this Addendum.

5. Vendor Employee Training

Vendor agrees that any of its officers or employees, and any officers or employees of any Assignee of Vendor, who have access to Protected Information will receive training on the federal and state law governing confidentiality of such information prior to receiving access to that information.

6. No Use of Protected Information for Commercial or Marketing Purposes

Vendor warrants that Protected Information received by Vendor from BOCES or by any Assignee of Vendor, shall not be sold or used for any commercial or marketing purposes; shall not be used by Vendor or its Assignees for purposes of receiving remuneration, directly or indirectly; shall not be used by Vendor or its Assignees for advertising purposes; shall not be used by Vendor or its Assignees to develop or improve a product or service; and shall not be used by Vendor or its Assignees to market products or services to students.

7. Ownership and Location of Protected Information

7.1. Ownership of all Protected Information that is disclosed to or held by Vendor shall remain with BOCES. Vendor shall acquire no ownership interest in education records or Protected Information.

7.2. BOCES shall have access to the BOCES's Protected Information at all times through the term of this Contract. BOCES shall have the right to import or export Protected Information in piecemeal or in its entirety at their discretion, without interference from Vendor.

7.3. Vendor is prohibited from data mining, cross tabulating, and monitoring data usage and access by BOCES or its authorized users, or performing any other data analytics other than those required to provide the Product to BOCES. Vendor is allowed to perform industry standard back-ups of Protected Information. Documentation of back-up must be provided to BOCES upon request.

7.4. All Protected Information shall remain in the continental United States (CONUS) or Canada. Any Protected Information stored, or acted upon, must be located solely in data centers in CONUS or Canada. Services which directly or indirectly access Protected Information may only be performed from locations within CONUS or Canada. All helpdesk, online, and support services which access any Protected Information must be performed from within CONUS or Canada.

8. Purpose for Sharing Protected Information

The exclusive purpose for which Vendor is being provided access to Protected Information is to provide the product or services that are the subject of this Contract to Wayne-Finger Lakes BOCES/EduTech.

9. Downstream Protections

Vendor agrees that, in the event that Vendor subcontracts with or otherwise engages another entity in order to fulfill its obligations under this Contract, including the purchase, lease, or sharing of server space owned by another entity, that entity shall be deemed to be an "Assignee" of Vendor for purposes of Education Law Section 2-d, and Vendor will only share Protected Information with such entities if those entities are contractually bound to observe the same obligations to maintain the privacy and security of Protected Information as are required of Vendor under this Contract and all applicable New York State and federal laws.

10. Protected Information and Contract Termination

10.1. The expiration date of this Contract is defined by the underlying contract.

10.2. Upon expiration of this Contract without a successor agreement in place, Vendor shall assist BOCES in exporting all Protected Information previously received from, or then owned by, BOCES.

10.3. Vendor shall thereafter securely delete and overwrite any and all Protected Information remaining in the possession of Vendor or its assignees or subcontractors (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies of shared data) as well as any and all Protected Information maintained on behalf of Vendor in secure data center facilities.

10.4. Vendor shall ensure that no copy, summary or extract of the Protected Information or any related work papers are retained on any storage medium whatsoever by Vendor, its subcontractors or assignees, or the aforementioned secure data center facilities.

10.5. To the extent that Vendor and/or its subcontractors or assignees may continue to be in possession of any de-identified data (data that has had all direct and indirect identifiers removed) derived from Protected Information, they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party.

10.6. Upon request, Vendor and/or its subcontractors or assignees will provide a certification to BOCES from an appropriate officer that the requirements of this paragraph have been satisfied in full.

11. Data Subject Request to Amend Protected Information

11.1. In the event that a parent, student, or eligible student wishes to challenge the accuracy of Protected Information that qualifies as student data for purposes of Education Law Section 2-d, that challenge shall be processed through the procedures provided by the BOCES for amendment of education records under the Family Educational Rights and Privacy Act (FERPA).

11.2. Vendor will cooperate with BOCES in retrieving and revising Protected Information, but shall not be responsible for responding directly to the data subject.

12. Vendor Data Security and Privacy Plan

12.1. Vendor agrees that for the life of this Contract the Vendor will maintain the administrative, technical, and physical safeguards described in the Data Security and Privacy Plan set forth in Attachment C to this Contract and made a part of this Contract.

12.2. Vendor warrants that the conditions, measures, and practices described in the Vendor's Data Security and Privacy Plan:

12.3. align with the NIST Cybersecurity Framework 1.0;

12.4. equal industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection;

12.5. outline how the Vendor will implement all state, federal, and local data security and privacy contract requirements over the life of the contract, consistent with the BOCES data security and privacy policy (Attachment B);

12.6. specify the administrative, operational and technical safeguards and practices it has in place to protect Protected Information that it will receive under this Contract;

12.7. demonstrate that it complies with the requirements of Section 121.3(c) of this Part;

12.8. specify how officers or employees of the Vendor and its assignees who have access to Protected Information receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;

12.9. specify if the Vendor will utilize sub-contractors and how it will manage those relationships and contracts to ensure Protected Information is protected;

12.10. specify how the Vendor will manage data security and privacy incidents that implicate Protected Information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify BOCES; and

12.11. describe whether, how and when data will be returned to BOCES, transitioned to a successor contractor, at BOCES's option and direction, deleted or destroyed by the Vendor when the contract is terminated orexpires.

13. Additional VendorResponsibilities

Vendor acknowledges that under Education Law Section 2-d and related regulations it has the following obligations with respect to any Protected Information, and any failure to fulfill one of these statutory obligations shall be a breach of this Contract:

13.1 Vendor shall limit internal access to Protected Information to those individuals and Assignees or subcontractors that need access to provide the contracted services;

13.2 Vendor will not use Protected Information for any purpose other than those explicitly authorized in this Contract;

13.3 Vendor will not disclose any Protected Information to any party who is not an authorized representative of the Vendor using the information to carry out Vendor's obligations under this Contract or to the BOCES unless (1) Vendor has the prior written consent of the parent or eligible student to disclose the information to that party, or (ii) the disclosure is required by statute or court order, and notice of the disclosure is provided to BOCES no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order;

13.4 Vendor will maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Protected Information in its custody;

13.5 Vendor will use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the secretary of the U S. Department of HHS in guidance issued under P.L. 111-5, Section 13402(H)(2);

13.6 Vendor will notify the BOCES of any breach of security resulting in an unauthorized release of student data by the Vendor or its Assignees in violation of state or federal law, or of contractual obligations relating to data privacy and security in the most expedient way possible and without unreasonable delay but no more than seven calendar days after the discovery of the breach; and

Where a breach or unauthorized disclosure of Protected Information is attributed to the Vendor, the Vendor shall pay for or promptly reimburse BOCES for the full cost incurred by BOCES to send notifications required by Education Law Section 2-d.

Signatures

For Wayne-Finger Lakes BOCES/EduTech	For (Vendor Name) **Pathful, Inc.**
Date 4/25/23	**Date** **April 19, 2023**

Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

Attachment A – Parent Bill of Rights for Data Security and Privacy

Wayne-Finger Lakes BOCES (EduTech)

Parents' Bill of Rights for Data Privacy and Security

The Wayne-Finger Lakes BOCES (EduTech)seeks to use current technology, including electronic storage, retrieval, and analysis of information about students' education experience in the BOCES, to enhance the opportunities for learning and to increase the efficiency of our BOCES and school operations.

The Wayne-Finger Lakes BOCES (EduTech)seeks to insure that parents have information about how the BOCES stores, retrieves, and uses information about students, and to meet all legal requirements for maintaining the privacy and security of protected student data and protected principal and teacher data, including Section 2-d of the New York State Education Law.

To further these goals, the Wayne-Finger Lakes BOCES (EduTech) has posted this Parents' Bill of Rights for Data Privacy and Security.

1. A student's personally identifiable information cannot be sold or released for any commercial purposes.
2. Parents have the right to inspect and review the complete contents of their child's education record. The procedures for exercising this right can be found in Board Policy 5500 entitled Family Educational Rights and Privacy Act (FERPA).
3. State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.
4. A complete list of all student data elements collected by the State is available at http://www.nysed.gov/data-privacy-security/student-data-inventory and a copy may be obtained by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.
5. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to the Chief Privacy Officer, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

Revised October 2019

Signatures

For Wayne-Finger Lakes BOCES/EduTech	For (Vendor Name) Pathful, Inc.
[signature]	[signature]
Date 4/21/23	Date April 19, 2023

Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

Attachment B – Wayne-Finger Lakes BOCES/EduTech Data Privacy and Security Policy

In accordance with New York State Education Law §2-d, the BOCES hereby implements the requirements of Commissioner's regulations (8 NYCRR §121) and aligns its data security and privacy protocols with the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (NIST Cybersecurity Framework or "NIST CSF").

In this regard, every use and disclosure of personally identifiable information (PII) by the BOCES will benefit students and the BOCES (for example, improving academic achievement, empowering parents and students with information, and/or advancing efficient and effective school operations). PII will not be included in public reports or other documents.

The BOCES also complies with the provisions of the Family Educational Rights and Privacy Act of 1974 (FERPA). Consistent with FERPA's requirements, unless otherwise permitted by law or regulation, the BOCES will not release PII contained in student education records unless it has received a written consent (signed and dated) from a parent or eligible student. For more details, see Policy 6320 and any applicable administrative regulations.

In addition to the requirements of FERPA, the Individuals with Disabilities Education Act (IDEA) provides additional privacy protections for students who are receiving special education and related services. For example, pursuant to these rules, the BOCES will inform parents of children with disabilities when information is no longer needed and, except for certain permanent record information, that such information will be destroyed at the request of the parents. The BOCES will comply with all such privacy provisions to protect the confidentiality of PII at collection, storage, disclosure, and destruction stages as set forth in federal regulations 34 CFR 300.610 through 300.627.

The Board of Education values the protection of private information of individuals in accordance with applicable law and regulations. Further, the BOCES Director of Educational Technology is required to notify parents, eligible students, teachers and principals when there has been or is reasonably believed to have been a compromise of the individual's private information in compliance with the Information Security Breach and Notification Act and Board policy and New York State Education Law §2-d

a) "Private information" shall mean **personal information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired:

1. Social security number.
2. Driver's license number or non-driver identification card number; or
3. Account number, credit or debit card number, in combination with any required security code, access code, or password, which would permit access to an individual's financial account.
4. Any additional data as it relates to administrator or teacher evaluation (APPR)

"Private information" does not include publicly available information that is lawfully made available to the general public from federal, state or local government records.

**"Personal information" shall mean any information concerning a person, which, because of name, number, symbol, mark or other identifier, can be used to identify that person.

b) Personally Identifiable Information, as applied to student data, means 40 personally identifiable information as defined in section 99.3 of Title 34 of the Code of 41 Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 42 U.S.C 1232-g, and as applied to teacher and principal data, means personally 43 identifying information as such term is defined in Education Law §3012-c(10).

c) Breach means the unauthorized access, use, or disclosure of student data 9 and/or teacher or principal data. Good faith acquisition of personal information by an employee or agent of the BOCES for the purposes of the BOCES is not a breach of the security of the system, provided that private information is not used or subject to unauthorized disclosure.

Notification Requirements
Methods of Notification

The required notice shall be directly provided to the affected persons and/or their guardians by one of the following methods:

a) Written notice;

b) Secure electronic notice, provided that the person to whom notice is required has expressly consented to receiving the notice in electronic form; and a log of each such notification is kept by the BOCES when notifying affected persons in electronic form. However, in no case shall the BOCES require a person to consent to accepting such notice in electronic form as a condition of establishing any business relationship or engaging in any transaction;

Regardless of the method by which notice is provided, the notice shall include contact information for the notifying BOCES and a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so acquired. This notice shall take place 60 days of the initial discovery.

In the event that any residents are to be notified, the BOCES shall notify the New York State Chief Privacy Officer, the New York State Cyber Incident Response Team, the office of Homeland Security, and New York State Chief Security Officer as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected residents.
The Superintendent or his/her designee will establish and communicate procedures for parents, eligible students, and employees to file complaints about breaches or unauthorized releases of student, teacher or principal data (as set forth in 8 NYCRR §121.4). The Superintendent is also authorized to promulgate any and all other regulations necessary and proper to implement this policy.

Data Protection Officer

The BOCES has designated a BOCES employee to serve as the BOCES's Data Protection Officer.

The Data Protection Officer is responsible for the implementation and oversight of this policy and any related procedures including those required by Education Law Section 2-d and its implementing regulations, as well as serving as the main point of contact for data privacy and security for the BOCES.

The BOCES will maintain a record of all complaints of breaches or unauthorized releases of student data and their disposition in accordance with applicable data retention policies, including the Records Retention and Disposition Schedule ED-1 (1988; rev. 2004).

Annual Data Privacy and Security Training

The BOCES will annually provide data privacy and security awareness training to its officers and staff with access to PII. This training will include, but not be limited to, training on the applicable laws and regulations that protect PII and how staff can comply with these laws and regulations.

References:

Education Law §2-d

8 NYCRR §121

Family Educational Rights and Privacy Act of 1974, 20 USC §1232(g), 34 CFR 99

Individuals with Disabilities Education Act (IDEA), 20 USC §1400 et seq., 34 CFR 300.610–300.627

Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

Attachment C – Vendor's Data Security and Privacy Plan

The Wayne-Finger Lakes BOCES Parents Bill of Rights for Data Privacy and Security, which is included as Attachment B to this Addendum, is incorporated into and make a part of this Data Security and Privacy Plan.

(Vendor can attached)

Pathful connect

Nepris Privacy Policy

Last Updated: September 15, 2022

Nepris Inc. ("Nepris) is a wholly owned subsidiary of Pathful, Inc. ("Pathful"). Some or all of the Services or Platform (as defined below) may be provided by Nepris or Pathful, and in the case they are provided by Pathful, all references to Nepris shall be deemed to include Pathful.

1. What Information Does Nepris Collect?

We take the information you provide to us very seriously, and we strive to put you in control of decisions around your information.

Our website is adopted mainly by K-12 school districts and affiliated schools and their teachers (collectively, "Schools") for the benefit of their students ("Student" or "Students"), including some Students that may be under of the age of thirteen ("Child User" or "Child Users").

The main features of our website include the following: (1) live video sessions of an industry expert interacting with a classroom at the request of a teacher ("Live Session"); (2) presentations by a company, organization, or industry expert to one or more classrooms ("Industry Chats"); and (3) the on-demand video library in which all recorded Live Sessions and Industry Chats reside ("Video Library"). Live Sessions, Industry Chats and the Video Library, together will all other features, software and services of the Nepris website are referred to collectively as the "Platform."

You can use some features of the Platform without registering for an account or providing any other personal information. If you create an account on the Platform, or communicate with Nepris, you may provide Nepris what is generally called "Personal Information" or "Personal Data," such as your full name, birthdate, email address or other information that can be used to identify you. Information that cannot be used to identify you as an individual is "de-identified" or non-personal information.

We collect information, including personal information, in a variety of ways which may vary according to your use of the Service and your account settings. The categories of personal information we collect may include:

- Contact and profile information
- Account and authentication information from third-party integrated services
- Approximate location information inferred from your IP address
- Information about your browser or device
- Non-personal information that may be linked to your Personal Information

Below, we describe examples of the categories of information we collect from and about you when you use our Platform:

a. Contact and profile information.

When you create an account on the Platform, or communicate with us, we may collect personal information including your name, email address, and birthdate. After you register, you may also choose to provide additional information in your profile, such as your headline, location (city), and other personal or demographic information. In addition, we may ask you for Personal Information at other times, such as when you contact our technical support team, send us an email, complete a user survey, or otherwise communicate with Nepris. We will share the email addresses of Event presenters to Event administrators to facilitate communication with respect to, and organization of, Events.

b. Information from Integrated Sign-On Platforms.

If you decide to register through or otherwise grant access to a third-party social networking or integrated service (what we call an "Integrated Platform"), such as Classlink, Google, LinkedIn or similar single sign-on service, Nepris may also collect Personal Information that is already associated with your Integrated Platform account. You may also have the option of sharing additional information with Nepris through an Integrated Platform, as controlled through your settings on that Integrated Platform. If you choose to provide such information, during registration or otherwise, Nepris will treat the information as Personal Information and will use it in the ways described in this Privacy Policy.

c. Information obtained from other users.

We make available certain features on our Platform that allow other users to provide us information about you. For example, a teacher may provide information relating to a Student, such as name, Student ID, date of birth, grade, class, and email address.

d. Information provided by partners and other sources.

We may also receive information from third-party organizations with whom we partner to provide educational services. If we combine or associate information from other sources with Personal Information that we collect through our Platform, we will treat the combined information as Personal Information in accordance with this Privacy Policy. For industry experts referred to Nepris via LinkedIn, we obtain name and LinkedIn profile data from LinkedIn. Schools and school districts for whom we provide services or rostering services (such as Classlink) with whom we partner may provide information relating to a Student, such as name, Student ID, date of birth, grade, class, and email address.

e. Information about your use of our Platform.

We may collect usage information about your use of our Platform, such as signing up for an Industry Chat, the number of videos you have viewed, using lesson plans, participation in message boards, and other ways in which our Platform can be used. This information enables us to better tailor educational experiences that are most appropriate for you.

f. Location information.

We may collect and use information about your location (such as your country) or infer your approximate location based on your IP address in order to provide you with tailored educational experiences for your region, but we don't collect the precise geolocation of you or your device. You may be able to change the settings on your computer or mobile device to prevent it from providing us with any location information.

g. Video session data.

Schools, industry experts, companies and organizations provide Nepris with permission to record both video and audio of every Live Session and Industry Chat to add to the Video Library. Nepris ensures that no Student images are retained in any form in these recordings. If Student voices are retained, personally identifiable information is removed.

Schools, industry experts, companies and organizations may request that a video file or associated content, such as documents and presentations (the "Content"), be deleted from the video library by emailing a request to nepris@nepris.com. You must be able to identify the particular Content you wish to be deleted or de-identified so that we can locate it on the Platform, and please note the reason that you are requesting the specific Content to be deleted. If you request that Content be deleted, Nepris will use reasonable efforts to remove it from the Platform, but you acknowledge that caching or references to the Content may not be made immediately unavailable. Also, please note that removal of your Content or information does not ensure complete or comprehensive removal, as there may be de-identified or recoverable elements of your content or information on our servers in some form. Additionally, we will not remove content or information that we may be required to retain under applicable federal and state laws.

2. How Does Nepris Use Collected Information?

a. To provide and enhance our Platform.

Nepris uses the information you provide or that we collect to operate, maintain, enhance, and provide all of the features of our Platform.

The most common user scenario for Nepris live sessions and industry chats is as follows: The classroom teacher who requested a live session or registered for an industry chat logs into the Platform and controls the classroom computer, which is typically the only live feed in the classroom, and there is no need for individual Students to login from their own devices. In this scenario, a video feed of the classroom and Students may be visible to the presenter depending on where the video camera is positioned within the classroom. The industry expert/presenter will be able to hear the voice of any Student who asks a question or makes a comment out loud.

The name and video feed of a Student who joins a Live Session or Industry Chat from a remote location or on their own device (i.e., from home during a virtual classroom session) may be visible to the industry expert/presenter if the Student is using a computer or device in which a third-party video platform integrated with Nepris ("Third-party Video Platform") is installed and logged in. The name of the session attendee is typically derived from the Nepris login used to access the meeting, but note, however, if the user already has the Third-party Video Platform installed account on that computer or device and is logged in, the Third-party Video Platform may automatically use the login information from the installed Third-party Video Platform.

Before Live Sessions and Industry Chats are placed into the Video Library, Nepris ensures that no Student images or spoken or displayed names are retained in any form in the recordings. If voices are retained, personally identifiable information is removed.

b. To personalize your experience.

We use the information to personalize your experience while using the Platform, including on various devices you may use to access the Platform. For instance, Nepris remembers your recent activity so we can recommend the most appropriate content for you on your next visit and provide personalized learning experiences.

c. To communicate with you.

We use your information to communicate with you about your account and respond to inquiries. We may also use your Personal Information to provide you with information about Nepris's features, services, upgrades, and other offerings that may be of interest to you.

d. To understand, improve, and develop our Platform.

Nepris uses all of the information that you provide or that we collect from users to understand and analyze the usage trends, learning behaviors, and preferences of our users, to improve the way the Platform works and looks, and to create new features and functionality. We may also use information to maintain, develop, support and improve our Platform and other educational products and services.

e. To enable your participation in Nepris partnership arrangements.

We use your information to enable your participation in programs or features we may offer in partnership with third parties, to the extent you wish to participate in such programs.

f. To log you in to the Third-party Video Platform or the Video Library.

We use your information to log you into the Third-party Video Platform that we use so that you are directed to the live feed that you have permission to access, and to log you into the Video Library, so that we know you have permission to access the Video Library.

For personal data subject to the European Union General Data Processing Regulations ("GDPR"), we rely on several legal bases to process the data. These legal bases include where:

- The processing is necessary to perform our contractual obligations in our Terms of Platform or other contracts with you (such as to provide you the Platform as described in our Terms of Platform);
- You have given your prior consent, which you may withdraw at any time (such as for marketing purposes or other purposes we obtain your consent for from time to time);
- The processing is necessary to comply with a legal obligation, a court order or to exercise or defend legal claims;
- The processing is necessary for the purposes of our legitimate interests, such as in improving, personalizing, and developing the Platform, marketing the Platform, such as new features or products that may be of interest, and promoting safety and security as described above.

If you have any questions about or would like further information concerning the legal basis on which we collect and use your Personal Information, please contact us using the contact details provided below.

g. To create and expand our Video Library.

Unless otherwise instructed in accordance with our Terms of Service, we record all Live Sessions and Industry Chats, then edit them to delete any Personally Identifiable Information of Students, such as faces and names, and make the edited recordings available to all registered users to access on demand in our Video Library.

3. School Users and Student Records.

Nepris strives to implement best practices to protect the privacy of all of our Student and non-Student users, alike. To help our school partners address their obligations to protect their Students' data privacy, we have implemented additional controls and procedures for schools, school districts, teachers, and administrators (collectively referred to as "Schools") when they enter into a contract with Nepris to use the Platform as part of the School's educational curriculum. When the Platform is used as part of the School's educational curriculum,

the Personal Information related to the School's Student users ("School Users") that is (i) provided to Nepris by a Student or by a School, or (ii) collected by Nepris during the provision of the Platform to a School, may include information defined as "educational records" by the Family Educational Rights and Privacy Act ("FERPA") or other information protected by similar Student data privacy laws. We call this information "Student Records."

Please note, because some of our user accounts may be used for both School and non-School purposes, only Personal Information relating to user accounts which are (1) created by a School (for example, when a teacher creates the user name, login and password to establish School User accounts, or when the teacher rosters a class using Google Classroom, Clever, or similar single sign-on service), or (2) created by a School User at the direction of a School and using a School email address and associated with a School's class on the Platform, and (3) created pursuant to a contract between Nepris and the School, are designated as Student Records on Nepris. We structure our Third-Party Video Platform to use and display only the first initial/last name of the Student. However, if a School User is using a computer or device with an existing Third-Party Video Platform account (i.e., separate from the Platform) and is logged into that existing account while attempting to use the Platform in connection with School purposes, the Third-Party Video Platform may default to displaying the name associated with the existing account rather than the first initial/last name of the School User. We recommend logging out of the existing Third-Party Account and logging into the Platform separately in order to avoid the default name from being used from the concurrent Third-Party Video Platform logins. In all cases, we have attempted to limit the name of the School User to first initial and last name only. Nepris will remove any name associated with a School User in the final edited recording. If you are a School, please contact us at nepris@nepris.com to learn more about how to create School User accounts that may hold Student Records.

Our commitment: Our collection and use of Student Records is governed by our contracts with the Schools, by our Privacy Policy, and by applicable privacy laws. For example, we work with Schools to help protect Personal Information from the Student's educational record, as required by the Family Educational Rights and Privacy Act ("FERPA"), and to protect the Personal Information of Students under 13 consistent with the Children's Online Privacy Protection Act ("COPPA"). If you have any questions about reviewing, modifying, or deleting the Personal Information of a School User accessing the Platform through a School partner agreement, please contact your School directly.

- We collect, maintain, use and share Student Records only for authorized educational purposes and as described in our Privacy Policy, or as directed by the School, the School User and/or the Student's parent or legal guardian (a "Parent").
- We do not disclose Student Records for targeted advertising purposes.
- We do not build a personal profile of a School User other than in furtherance of an educational purpose or as authorized by a Parent.
- We maintain a comprehensive data security program designed to protect the types of Student Records maintained by the Platform.
- We will clearly and transparently disclose our data policies and practices to our users.
- We will never sell Student Records unless the sale is part of a corporate transaction, such as a merger, acquisition, bankruptcy, or other sale of assets, in which case we will require the new owner to continue to honor the terms provided in this Privacy Policy or we will provide the School with at least thirty (30) days notice and an opportunity to opt-out of the transfer of Student Records by deleting the Student Records before the transfer occurs.
- We will not make any material changes to our Privacy Policy or contractual agreements that relate to the collection or use of Student Records without first giving notice to the School and providing a choice before

the Student Records are used in a materially different manner than was disclosed when the information was collected.

a. How we share and disclose Student Records.

Depending on the features and account controls applicable to the School User accounts, we may share usernames and profile information with other users on the Platform, such as teachers or administrators.

Depending on the manner in which Nepris is used by a School and the terms of the agreement between the School and Nepris, Nepris may provide access to certain Student Records, School User account usage data ("School Analytics") and teacher user account usage data to the School for the purpose of monitoring Student usage and activity and evaluating the effectiveness of the School's use of the Nepris service. In some circumstances, School Analytics may only be available for Student accounts using a School email address or login and which are associated with a School's teacher.

b. How we retain and delete Student Records.

We keep Personal Information until it is deleted, or until we no longer need it to provide you with the Platform. We will not retain Student Personal Information for any longer than is necessary for education purposes and legal obligations, or to provide the Platform for which we receive or collect the Student Personal Information. In addition, we only keep Student Personal Information for as long as the Student account is active, unless we are required by law or the Student's school to retain or need it to protect the safety of our users. Note that some content may be kept after an account is deleted for school legal compliance reasons (e.g., maintenance of "education records" under FERPA or "Student records" under various state Student privacy laws).

All users, including School Users, can delete their accounts and all Personal Information associated with the account at any time by contacting us at nepris@nepris.com to request deletion of Student Records associated with the School's use of Nepris. Please note that Nepris cannot comply with a School's request to delete Personal Information in a user account except for School User accounts created by a School (i.e., using a School email address and/or an account login provided by or associated with a School) pursuant to a contractual agreement between the School and Nepris, or unless the School User (or the School User's Parent) requests deletion directly. The School is responsible for managing Student Records that the School no longer needs for an educational purpose by submitting a deletion request when such data is no longer needed. Schools should contact us at nepris@nepris.com.

c. Questions about Student Records.

If you have questions about specific practices relating to Student Records provided to Nepris by a School, please direct your questions to your School.

4. Nepris Children's Privacy Policy.

Nepris does not permit Child Users to create an account without the consent and at the direction of a Parent or School. When Nepris is used by a School in an educational setting, we may rely on the School to provide the requisite consent for Nepris to collect information from a Child Use in lieu of Parental consent.

Please contact us at nepris@nepris.com if you believe we have inadvertently collected information from a Child User without Parental consent or at the direction of a School so that we may delete the information as soon as possible.

Please see the Children's Privacy Policy to learn more about how Nepris collects, uses and shares information associated with Child User accounts.

5. Cookie Policy.

A "cookie" is a string of information that a website stores on a visitor's computer, and that the visitor's browser provides to the website each time the visitor returns. To provide a personalized learning and high-quality experience for our users, we may use various technologies that automatically record certain technical information from your browser or device when you visit our website, read our emails, use our Platform or otherwise engage with us. This information is typically collected through a variety of tracking technologies, including cookies, web beacons, Flash objects, log files, and similar technology (collectively, "tracking technologies"). Some cookies may be used to recognize the user viewing a particular website, make navigation easier, and customize the content. For example, cookies allow us to remember your actions and preferences so that you do not have to re-enter information each time you visit our site or navigate to another page.

These tracking technologies cookies collect information about how you use the Platform (e.g., the pages you view, the links you click, and other actions you take on the Platform), information about your browser and online usage patterns (e.g., Internet Protocol ("IP") address, browser type, browser language, referring / exit pages and URLs, pages viewed, whether you opened an email, links clicked), and information about the device(s) you use to access the Platform (e.g., mobile device identifier, mobile carrier, device type, model and manufacturer, mobile device operating system brand and model, and whether you access the Platform from multiple devices). We may collect analytics data, or use third-party analytics tools such as Google Analytics, to help us measure traffic and usage trends for the Sites and to understand more about the demographics of our users. You can learn more about Google's practices at http://www.google.com/policies/privacy/partners, and view its currently available opt-out options at https://tools.google.com/dlpage/gaoptout. We may also work with third-party partners to employ technologies, including the application of statistical modeling tools, which permit us to recognize and contact you across multiple devices. Although we do our best to honor the privacy preferences of our users, we are unable to respond to Do Not Track signals set by your browser at this time.

We use and/or one or more third-party services we work with may use the data collected through tracking technologies to better display our website, to save you time, to provide better technical support, for promotional purposes, and to track website usage. For example, cookies help us to:

1. Keep track of whether you are signed in or have previously signed in so that we can display all the features that are available to you.
2. Remember your settings on the pages you visit, so that we can display your preferred content the next time you visit.
3. Customize the function and appearance of the pages you visit based on information relating to your account; for example, in order to default you to a particular study level, or to remember customized settings for a report.
4. Track website usage for various purposes including informing site improvements, sales, marketing, and billing.

Most browsers are initially set up to accept cookies, but you can reset your browser to refuse all cookies or to indicate when a cookie is being sent. However, some features and services (particularly those that require you to sign-in) may not function properly if your cookies are disabled. You may also set your email options to prevent the automatic downloading of images that may contain technologies that would allow us to know whether you have accessed our email and performed certain functions with it.

Deleting cookies does not delete Local Storage Objects (LSOs) such as Flash objects and HTML5. You can learn more about Flash objects - including how to manage privacy and storage settings for Flash cookies – on Adobe's website or by clicking here. Various browsers may offer their own management tools for removing HTML5 LSOs. Please consult your browser's "Help" function to learn more. If you choose to delete Flash objects from our sites, then you may not be able to access and use all or part of the sites or benefit from the information and services offered.

6. Nepris Protection Measures.

Nepris takes great care to protect the information you provide us. We do not rent or sell Personal Information that we collect from users with third parties.

Nepris will disclose Personal Information when you consent or instruct us to share your Personal Information with third parties, or when we have a legitimate business or legal need to share your information. In addition, industry experts and teachers may have a public profile page that will reveal your full name and organization (school/school district or company), as well as a short bio, a photograph, and other information that you provide. Nepris will link to your public profile page when you post content that is visible to others on the Platform. Students do not have a public profile and other users cannot find, identify or contact them through the Platform. In addition, administrators of each of the paid groups using the Platform (such as school districts and their affiliated schools) will have access to the complete set of data for that group's users and activities. We may also disclose anonymous or aggregate information that does not reasonably identify you as an individual. To learn more, see additional description below.

a. When information is visible to others on the Platform by default.

Certain features and functions of the Platform shares or makes information of industry experts and teachers accessible to others. As with most online services, once you make your Personal Information available to others online, it may be collected and used by the recipients or any other website visitor without restriction. Industry experts and teachers can create public profiles that are visible to other users. Public profiles may include your name, short biography and city-level location. This information may be visible when you post a question or comment to the Platform. Students may post a question or comment to the Platform but their Personal Information is not included. Nepris reviews user questions and comments before making them public.

b. With your consent or according to your instructions.

You may provide consent or authorization to share your Personal Information with third-party applications or services in several ways. Please note that these third parties are not governed by Nepris or the terms of this Privacy Policy. We recommend you review the privacy policy of any third-party application or service before authorizing access to your Nepris account information.

- We may share data with third-party applications that you authorize. Third-party application developers and service providers (commonly known as "App Developers") may build complementary services for our platform, such as a mobile application for visually impaired learners to access our resources or may use our Nepris content to build unaffiliated applications and services. If you connect your Nepris account to an application or service or approve access to your Nepris account by a third-party application or service, you consent to Nepris sharing your Personal Information with that third-party.

- We may share data in connection with special programs you participate in. If you participate in special programs where Nepris partners with third parties, Nepris may share data collected from or about you with

its third-party partners to facilitate the program or services being offered. These program partners may use your information we share with them as described in their own privacy policies.

- We may share information with your consent. Nepris does not share your Personal Information with third-party organizations for their marketing or promotional use without your consent. In some instances, you may be able to grant us permission to share your Personal Information with authorized partners, not-for-profit organizations, and other entities that are not affiliated with Nepris. In these cases, we will only provide to these third parties the information you have authorized or asked us to share to these third parties. You may also choose to share content with others by email, or by posting Nepris content to social media sites such as Facebook or Twitter. These third parties may use your information as described in their own privacy policies.

c. We may share anonymous or aggregate data with others.

We may use data which has been de-identified and/or aggregated for product development, research, analytics and other purposes, including for the purpose of analyzing, improving, or marketing the Platform. On certain occasions, Nepris may share this data with business partners to improve our services or offerings. If we disclose information to authorized business partners to conduct research on online education or assist in understanding the usage, viewing, and demographic patterns for certain programs, content, services, promotions, and/or functionality on our Platform, such data will be aggregated and/or anonymized to reasonably avoid identification of a specific individual.

d. Other instances where we may share or disclose information for legal or business purposes.

- We will share data with employees and service providers. Nepris may share information with our employees and trusted vendors, third-party service providers and other individuals to provide services or products for us or on our behalf, which could include analytics, hosting, marketing and similar services. The list of these vendors and third-party service providers can be accessed here. When we share Personal Information with third-party service providers or vendors, these third parties are contractually obligated to maintain the security and confidentiality of that Personal Information.

- We may share data in the context of a change of business, including a merger or acquisition. In the event that Nepris is involved in a merger, acquisition, bankruptcy, change of control, or any form of sale of some or all of our assets, your Personal Information may be transferred or disclosed in connection with such a business transaction. If the transaction involves the transfer of Student Records to a third-party, we will require the new owner to continue to honor the terms provided in this Privacy Policy, or we will provide the School with at least thirty (30) days notice and an opportunity to opt-out of the transfer of Student Records by deleting Student Records before the transfer occurs.
- Other instances. Nepris may release Personal Information if we have a good faith belief that access, use, preservation, or disclosure of such information is reasonably necessary to (a) satisfy any applicable law, regulation, legal process, or enforceable governmental request; (b) enforce applicable Terms of Service, including investigation of potential violations thereof; (c) investigate and defend ourselves against any third-party claims or allegations; (d) detect, prevent or otherwise address fraud, security or technical issues; (e) protect the rights, property, or personal safety of Nepris, our users, or the public; or (f) as required or permitted by law.

7. Nepris Use of Information for Marketing.

a. Messages from Nepris.

We may, from time to time, send you email regarding our products and services, or other third-party products and services we think you may enjoy. For example, if we partner with a not-for-profit organization running a contest in your region we may send you an email notifying you of the partnership or contest. We will not share your information with the third-party unless you opt-in to participate in the partnership or contest, and if so, the information we would share would be limited to that needed to facilitate your participation in the contest and enable you to redeem your prize. You can unsubscribe from these mailings at any time. See Section 6 below.

b. Sponsored Content.

Nepris does not display any third-party advertisements on the Platform. From time to time, we may permit third parties to sponsor content displayed on our Platform. For example, for-profit organizations may wish to sponsor all content related to a particular educational topic. Sponsored content will always be labeled (e.g., "Sponsored by ___"). Nepris does not share any of our users' Personal Information with these sponsors without explicit consent, and these sponsors do not have the ability to track or collect information about our site visitors or users.

Please note: From time to time, we may display YouTube video content created by third-parties and not by Nepris. While Nepris-created video content does not display video advertisements, third-party content may include advertising, which we cannot control.

8. Third Parties and Online Advertising.

a. Interest-Based Advertising.

Nepris does not display any targeted advertising on our Platform. However, we participate in interest-based advertising and use third-party advertising companies to serve advertisements on other websites, apps or services, including on Facebook and other social networks, or on other devices you may use. We do not use any of your Personal Information for targeted advertising.

b. YouTube and other Video Providers.

Nepris may use services such as YouTube, Vimeo, Microsoft Video-Indexer and Media Platforms to display certain video content on the Platform. One or more of these services incorporates tracking technologies, which may be present in the videos embedded on the Platform, which may collect information from your browser when you view the video on the Platform, including device identifiers and/or cookie IDs.

This information is collected directly and automatically by the services and its partners, and Nepris does not participate in these data transmissions. Nepris does not provide any Personal Information, such as usernames, to YouTube or these other services.

9. User Control Over Data Collection and Management Preferences.

At Nepris, we use Personal Information as needed for the purposes for which it was collected or where you have consented to our use of your Personal Information. We take reasonable steps to ensure that the Personal Information that we store and use is accurate, complete, and up-to-date. If you discover that Personal Information or other data pertaining to you is inaccurate, incomplete, or out-of-date, please update your account information or contact us as outlined below.

a. You can choose to not provide us with Personal Information.

You may always decline to provide your Personal Information with Nepris. Registration is not required to access some of our online resources. If you decline to register, however, Nepris will not be able to provide you with certain features and functionalities found on our Platform. You may later enable or access those features by providing Nepris with the necessary Personal Information.

b. You can unsubscribe from email communications.

Nepris may, from time to time, send you email regarding our products and services, or products and services we think you may enjoy. Only Nepris (or our vendors or service providers operating on our behalf) will send you these emails. You can choose not to receive these emails by clicking the unsubscribe link in the footer of these emails. Please note that you are not permitted to unsubscribe or opt-out of non-promotional messages regarding your account, such as account verification, taking certain actions within the platform such as scheduling sessions, changes or updates to features of the Platform, or technical or security notices.

c. California Children's Privacy Rights.

If you are under the age of 18 residing in California, you are entitled to request removal of content or information you have posted publicly on our Platform. To delete your entire account and remove all of your information displayed publicly on the Platform, or to request deletion or de-identification of a specific question, answer or other post displayed publicly on the Platform, please email us at nepris@nepris.com for assistance. You must be able to identify the particular post you wish to be deleted or de-identified so that we can locate it on the Platform. Please note that removal of your content or information does not ensure complete or comprehensive removal, as there may be de-identified or recoverable elements of your content or information on our servers in some form. Additionally, we will not remove content or information that we may be required to retain under applicable federal and state laws.

10. User Control Over Collected Information.

a. How to access or update your information.

We want you to have access to your information, so that you can help keep it as accurate as possible. If you register and provide Nepris with Personal Information, you may update, correct, or delete your account and information at any time by reviewing your profile information and preferences on your account settings page.

Parents can request that Nepris modify or delete Child User accounts by emailing us at nepris@nepris.com. Parents who request to modify or delete Student accounts may be directed to contact the School.

Nepris will work with schools to provide Parents access to information in School User accounts at the request and direction of the School. If you experience any difficulties in this process, please contact us as described below.

b. How to delete your information.

To request deletion of your Personal Information and/or videos, send an email to nepris@nepris.com setting forth your request. You can learn more in our Help Center, https://help.nepris.com Please note that your information will be retained in backup for up to one week.

In the event that you request that we remove content from Google index, we will delete that content from our site within a reasonable time and also request that Google remove the links to that content. Please note,

however, that this process is not immediate and we cannot provide a precise number of days by which the requested content will be removed from Google index.

We may not be able to delete data in all instances, such as information retained in technical support logs and other business records. We will not be required to delete any information which has been de-identified or disassociated with personal identifiers such that it can no longer be used to reasonably identify a particular individual.

Unless we receive a deletion request, we will retain your information for as long as your account is active or as is reasonably useful for operational purposes. For example, we may retain certain data as necessary to prevent fraud or future abuse, for recordkeeping or other legitimate business purposes, or if required by law. We may also retain information which has been de-identified or aggregated such that it can no longer reasonably identify a particular individual. All retained Personal Information will remain subject to the terms of this Privacy Policy.

11. Nepris Data Security Policy.

a. Data security is important to you, and to us.

To protect your privacy and security, we take reasonable steps to verify your identity before granting you account access or making corrections to your information. For example, we may ask you to provide certain Personal Information to confirm your identity, and we may require that you create and use a password to access certain parts of our Platform. You should create and maintain a strong password to help ensure the security of your account.

b. We try to ensure that our Platform and information sent to us are safe, but no security measures are perfect.

Nepris uses certain physical, managerial, and technical safeguards designed to preserve the integrity and security of your Personal Information and other information we maintain in connection with our Platform. We cannot, however, ensure or warrant the security of any or all of the information you transmit to Nepris, and you do so at your own risk. Once we receive your transmission of information, Nepris makes commercially reasonable efforts to ensure the security of our systems. When you enter sensitive information, we encrypt the transmission of that information using secure socket layer technology (SSL) or similar technologies. However, please note that this is not a guarantee that such information may not be accessed, disclosed, altered, or destroyed by breach of any of our physical, technical, or managerial safeguards. If Nepris becomes aware of a systems security breach by an unauthorized party or that any user data was used for an unauthorized purpose, we will comply with relevant state and other data breach laws. We will notify users of any breach resulting in unauthorized release of data electronically, at minimum, and without unreasonable delay so that you can take appropriate steps. The notification will include the following: date of the breath, the types of information that were subject to the breach, general description of what occurred, and steps Nepris is taking to address the breach.

12. California Users.

Nepris is not subject to regulation under the California Consumer Privacy Act of 2018 ("CCPA"). Therefore, even if you are a California resident and we may have Personal Information about you that is the type of the information subject to the CCPA, the CCPA is not applicable to Nepris or to our relationship with you. However, if you are a resident of the State of California and Nepris has an established business relationship with you,

then, pursuant to Section 1798.83 of the California Civil Code, you have the right to request the following at any time: (a) information from Nepris free of charge regarding the manner in which Nepris shares certain Personal Information collected through the Platform with third parties who use such information for direct marketing purposes; and (b) the discontinuation (or opt-out) of Nepris sharing of such information with such third parties. Please submit any such request ("California Privacy Rights Request") to any one of the following:

By mail: Pathful, Inc., 750 N Saint Paul St Ste 250, PMB 63880, Dallas, TX 75201-3206 , with a subject line of "Your California Privacy Rights."

By email: nepris@nepris.com, with a subject line of "Your California Privacy Rights."

For each California Privacy Rights Request, please state "Your California Privacy Rights" in the email or letter subject line, and clearly state the following in the body:

a. the nature of your request;

b. that the request is related to "Your California Privacy Rights;"

c. your name, street address, city, state, zip code and email address; and

d. whether you prefer to receive a response to your request by mail or email.

If you send a California Privacy Rights Request by mail, then please do so by U.S. Certified Mail, Return Receipt Requested to allow for confirmation of mailing, delivery and tracking. Nepris will not accept a California Privacy Rights Request via telephone or fax and is not responsible for a California Privacy Rights Request that is incomplete, incorrectly labeled or incorrectly sent.

You are solely responsible for the accuracy and content of your Personal Information, and for keeping your Personal Information current and correct.

13. International Visitors and Control Over Data.

We are headquartered in the United States of America. Personal Data may be accessed by us or transferred to us in the United States. The European Commission has not determined that the United States ensures an adequate level of protection for Personal Data.

If you choose to use our Platform from the European Union or other regions of the world with laws governing data collection and use that differ from United States law, then you acknowledge that Nepris will transfer your Personal Information to the United States for the purpose of performing the Platform according to our contract (e.g., our Terms of Service) and for any other purpose for which you provide explicit, informed consent.

By providing us with Personal Information, you consent to the storage or processing of your Personal Information in the United States and acknowledge that the Personal Information will be subject to the laws of the United States, including the ability of governments, courts or law enforcement or regulatory agencies of the United States to obtain disclosure of your Personal Data.

We will protect the privacy and security of Personal Information according to this Privacy Policy, regardless of where it is processed or stored.

14. Canadian Privacy Rights

If you are a Canadian Citizen, then, pursuant to Principle 9 of the Model Code for the Protection of Personal Information, you have the right to request the existence, use and disclosure of your Personal Information and be given access to that information. You are further able to challenge the accuracy and completeness of the information and have it amended as appropriate. Specifically, you are entitled to obtain free of charge, information from us regarding whether or not we have any of your Personal Information, an account of the use that has been made of that information, and an account of the third parties to which it has been disclosed. Please submit any such request ("Canada Privacy Rights Request") to any one of the following:

By mail: Pathful Inc., Attn. Canada Privacy Agent, 750 N Saint Paul St Ste 250, PMB 63880, Dallas, TX 75201-3206, with a subject line of "Your Canada Privacy Rights."

By email: nepris@nepris.com with a subject line of "Your Canada Privacy Rights – Attn. Canada Privacy Agent."

For each Canada Privacy Rights Request, please state "Your Canada Privacy Rights" in the email or letter subject line, and clearly state the following in the body: (a) the nature of your request; (b) that the request is related to "Your Canada Privacy Rights;" (c) your name, street address, city, state, zip code and email address; and (d) whether you prefer to receive a response to your request by mail or email. If you send a Canada Privacy Rights Request by mail, then please do so by U.S. Certified Mail, Return Receipt Requested to allow for confirmation of mailing, delivery and tracking. We will not accept a Canada Rights Request via telephone or fax and are not responsible for a Canada Privacy Rights Request that is incomplete, incorrectly labeled or incorrectly sent. Finally, as explained further above, we do not authorize third parties to collect your Personal Information when you use the Site, except as expressly stated in this Privacy Policy. To the fullest extent permitted by law, we are not responsible for, and you hereby release us from, any and all liability which may arise from, such third parties' unauthorized collection of your Personal Information.

15. European Union Data Protection.

Residents in the European Union are entitled to certain rights with respect to Personal Information that we hold about them:

- Right of access and portability. The right to obtain access to your Personal Information, along with certain related information, and to receive that information in a commonly used format and to have it transferred to another data controller;
- Right to rectification. The right to obtain rectification of your Personal Information without undue delay where that Personal Information is inaccurate or incomplete;
- Right to erasure. The right to obtain the erasure of your Personal Information without undue delay in certain circumstances, such as where the Personal Information is no longer necessary in relation to the purposes for which it was collected or processed;
- Right to restriction. The right to obtain the restriction of the processing undertaken by us on your Personal Information in certain circumstances, such as where the accuracy of the Personal Information is contested by you, for a period enabling us to verify the accuracy of that Personal Information; and
- Right to object. The right to object, on grounds relating to your particular situation, to the processing of your Personal Information, and to object to processing of your Personal Information for direct marketing purposes, to the extent it is related to such direct marketing.

You may also have the right to make a complaint to the relevant Supervisory Authority. A list of Supervisory Authorities is available here: http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm. If you need further assistance regarding your rights, please contact us using the contact information provided below

and we will consider your request in accordance with applicable law. In some cases, our ability to uphold these rights for you may depend upon our obligations to process Personal Information for security, safety, fraud prevention reasons, compliance with regulatory or legal requirements, or because processing is necessary to deliver the services you have requested. Where this is the case, we will inform you of specific details in response to your request.

16. Links to Third-party Websites.

The Platform may link to and may be linked by websites operated by other entities or individuals. Some of these websites, such as the Nepris Facebook page, may be co-branded with our name or logo. This Privacy Policy does not apply to, and we cannot always control the activities of, such other third-party websites. You should consult the respective privacy policies of those third-party websites.

17. Changes and Updates to Privacy Policy.

Nepris may modify or revise this Privacy Policy from time to time. Nepris will notify users of any changes to our Privacy Policy by posting the revised Privacy Policy with an updated date of revision on our Platform or on this page. Your continued use of the Platform following an update constitutes your acceptance of the revised Privacy Policy. We will not make any material changes to our Privacy Policy that relate to the collection or use of Student Records without first giving notice to the School and providing a choice before Student Records are used in a materially different manner than was disclosed when the information was collected.

18. Contacting Nepris.

Please contact Nepris with any questions or comments.

By email: nepris@nepris.com

By mail: Pathful Inc.

750 N Saint Paul St Ste 250

PMB 63880

Dallas, TX 75201-3206
Phone: 1-888-908-4924

You may also wish to visit the FAQ and Help Center page, which hosts useful FAQs and information that you may find helpful.

Supplement A: Nepris Children's Privacy Policy

Nepris is committed to children's privacy.

Protecting the privacy of children is especially important to Nepris. For that reason, we created certain features designed to help protect Personal Information relating to Child Users. Nepris does not knowingly permit Child Users to register directly for our Platform without consent of Parent or School. If Nepris learns that Personal Information of a Child User has been collected on our Platform without Parental consent, then Nepris will take appropriate steps to delete this information. If you are a Parent and discover that your child under the age of 13 has a registered account with our Platform without your consent, please alert Nepris at nepris@nepris.com to request that we delete that child's Personal Information from our systems.

How children may register for and use our Platform.

Child Users can sign up for a Nepris account several ways.

1. When a Child User signs up for a Nepris Account we request Parental consent.

When a Child User registers for our Platform, we request a birth date, username, password, and a Parent's email address so that we can email the Child User's Parent in order to seek consent for the Child to use the Platform. Nepris does not ask the Child User for any more information than is necessary to provide the Platform to the Child User or to seek Parental consent. The Child User is permitted to use the Platform for seven (7) days through a Restricted Account (see below) while we notify the Parent for consent. If we do not receive Parental consent within 7 days, the Child User's Restricted Account is closed, and the Child's Personal Information is deleted from our systems

2. When a Child User account is created by a School, the School may provide consent.

When the Platform is used by School in the classroom for an educational purpose, we permit the School to create Child User accounts and to provide the requisite consent for Nepris to collect Personal Information of a Child User for this purpose in lieu of Parental consent. Schools may create a Child User account by adding Students to the Platform through Google Classroom, Classlink, or similar single sign-on service, or through a school integration mechanism, or a School may create logins/passwords for each individual Student. When Schools create accounts in this manner, we do not request additional consent from the Parent. However, when a School or other individual invites a Child User to join the Platform and connect to a teacher's class using a class code, we request Parental consent in the manner described below.

3. Methods for providing Parental consent.

Parents may provide consent for a Child User to use the Platform through a Restricted Account (explained below) by responding affirmatively to an email sent by Nepris to the Parent's email address provided by the Child User during registration. If we do not receive consent from the Parent within seven (7) days, the Child User's account will be closed and the Child's Personal Information is deleted from our systems. Restricted Accounts may access and use certain features of the Platform in a limited manner.

4. Restricted Accounts for Child Users.

Nepris attempts to restrict a Child User's access to certain features that could result in disclosure of the Child User's Personal Information. A Restricted Account limits sharing and displaying private information about the Child User in various ways.

For example, a Child User with a Restricted Account cannot:

- display Personal Information. Restricted Accounts show only the Child User's initials to anyone other than the user and do not include other Personal Information or profile data. Platform
- add or edit Personal Information associated with a Restricted Account. If a School provides roster information, they cannot edit their name, email, class or teacher.
- post to public discussion forums, or post questions or answers on lessons except with only their initials visible.
- receive marketing-related emails from Nepris, but they can receive "system-only" emails such as support emails, reminders, codes, etc.

- communicate with or share Personal Information with other users. Similarly, teachers cannot communicate with a Child User with a Restricted Account except to assign content for the Child User to view through the class.

5. What information do we collect from a Child User?

We collect a username, birthdate, and Parent's email address when a Child User registers for the Platform. We collect information about the Child User's use of the Platform as well as content the Child posts to the Platform. We also collect usage and device information, as described above. We use this information to provide the Platform to the Child User and for the purposes described in in our Privacy Policy's section "How we use the information we collect." We use the Parent's email address to communicate messages about the account.

6. How do we disclose information relating to a Child User?

As described above, Restricted Accounts have limited data sharing capabilities. A Student-created username is NOT shared with a teacher unless it's considered school data.

7. Third-party tracking and online advertising.

Nepris does not display any targeted advertising in the Platform. We do not disclose Personal Information of Child Users for direct marketing purposes or for targeted advertising purposes. While we do permit third-party advertising partners to operate on our Platform for the purpose of re-targeting, analytics and attribution services (See our Privacy Policy section "Third Parties and Online Advertising"), we take steps to disable third-party ad networks on webpages with child-directed content or when a Child User logs into a Restricted Account on the Platform.

8. How to access, modify and delete your Child's Personal Information.

A Parent may contact us at nepris@nepris.com to access or delete the Child User's account. Please note you will need the Child User's username, and we may take steps to authenticate your identity before we can provide access to the Restricted Account.

Third Party	Purpose	Information Shared
Microsoft	Azure cloud hosting, database, and storage, videos, and analytics.	Geo information, IP address and tracking – via analytics gathering.
Zoom	Video Meetings – User accounts created using Names	Names and Nepris Unique Identifier
Vimeo	Video Repository	Videos
Google	Google Analytics, Firebase database	Geo Information, IP Address & Tracking, Firebase stores videos for processing
Olark	Live Chat	Geo Information, IP & Tracking

Dropbox	Document and video project storage	Videos, documents
Digital Ocean	Hosting, Video processing	Videos
iContact	Email Campaign Manager	User List (names, email, profile information, etc.)
LinkedIn	Volunteer Opportunity Listing	Info about Session Requester, District, School, etc.
SalesForce	Customer Relationship Management system.	nepris.com data or sales and marketing leads. Student data is not collected.
Cirrus	Sync email and contact data from Google with Salesforce	Data from business communications. Student data is not collected.
Dataloader	Sync nepris.com data with Salesforce	Data from nepris.com. Student data is not collected.
Validity	Sync nepris.com data with Salesforce	Sync data between nepris.com and Salesforce. Student data is not collected.
Zapier	Transfer data between other tools	Sending and updating calendar invites, notifications for events, etc. Student data not is not collected.
ChurnZero	Bring together nepris.com, support, and Salesforce to track health of accounts	Contact for student data (name, email) may be passed to ChurnZero if they use a support channel directly.
Zendesk	Support platform for manage emails, chats and phone calls	Student data (name, email) may be collected if they use a support channel directly. Geo Information, IP & Tracking on chats.