Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

EDUTECH

Quill

CONTRACT ADDENDUM

Protection of Student Personally Identifiable Information

1. Applicability of This Addendum

The Wayne-Finger Lakes BOCES/EduTech) and Empirical **("Vendor")** are parties to a contract dated 10/16/2023 ("the underlying contract") governing the terms under which BOCES accesses, and Vendor provides, Access to ("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 Empirical Resol.

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) Empirical Resolution Inc.
	Finance & Operations Manager
Date 10/23/24	**Date** 10/16/2023

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)** Empirical Resolution Inc.
Date 10/24/23	**Date** 10/16/2023

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)

Empirical Resolution Inc. Privacy Policy

Updated on September 26, 2018

Empirical Resolution Inc. (d/b/a Quill.org) ("we" or "us"), values your privacy and we are committed to creating a secure environment across our services, including our application programming interface, website and other online services (collectively, our "Website"). We use the data we collect to provide users with a high quality engaging experience and fulfill our mission of creating an active learning environment and helping students take charge of their education. Because we gather certain types of information about the users of the Website, we believe you should fully understand the terms and conditions surrounding the use of the information we collect. The following discloses our information gathering and dissemination practices for our Website. Please make sure that you read the terms of this privacy and any privacy policies that you enter into with parties other than us, including your employer or educational institution, as those policies may also explain how your personal information is used by those parties.

Your use of our Website means that you specifically and expressly consent to all practices described below in this Privacy policy and our Terms of Service, as amended from time to time. Any information you provide to us or the Website, along with your use of the Website, is subject to the terms in this Privacy policy and our Terms of Service, as amended from time to time.

How data is used and collected:

Quill.org collects the following data about our users and their use of our Website.

- **Personal information.**
  By registering with or using the Website, you may provide to Quill.org what is generally called "personally identifiable information" (such as your email address, name) that can be used to identify you, as well as demographic information such as your age, gender and interests. Through the rest of this Privacy policy, such information will be referred to as "Personal Information."

- **User-provided information and information about use of website.**
  In addition to Personal Information, we may collect information about your use of certain Website features, such as the number of activities you have completed, your time spent on various activities, and your scores on various activities. This information allows us to make a better, more personalized experience and provides us with data that we use to improve the Website. We may also request information for purposes such as the provision of customer service and support, billing, network management, customer surveys, newsletter subscriptions, user group memberships, event registration and sponsorship, offers of related services, and other exchanges of information.
  We may make chat rooms, forums, message boards, and/or news groups available in certain areas of the Website. Please remember that any information that is disclosed in these areas becomes public information, and you should exercise caution when deciding to disclose your Personal Information.
  Any content you submit to, or make available on, the Website ("User-Created Content") shall be your property and you represent that such User-Created Content does not infringe on the intellectual property of any third party. You hereby grant us a perpetual, irrevocable, royalty-free, sublicenseable worldwide license to use and display such User-Created Content.

- **Information obtained from other users and third parties.**
  Some features on the Website may be used that allow other users or third parties to provide us information, some of which may be Personal Information. For example, a parent may register an account for their child and provide us with certain information, such as the child's name or one of our partners may send us information when you access our Website through their Website or service.

- **Technical information.**
  We may record technical information such as your Internet Protocol (IP) address, internet service provider, browser type, operating system, the dates and times the Website is visited, referring or exit pages, and other data which tracks users' access to the Website. This data may be analyzed for the aggregate trends they reveal about our users and how the users use the Website.

How we use this information:

- **To personalize and maximize learning experiences.**

The information provided may be used to better your experience on the Website. For example, we may track which activities need to be finished and which ones are completed, and then use this information to suggest areas you may wish to work on.

- **To understand how users engage with the Website.**
  We use information provided by, or collected from, users to create new features, analyze trends and metrics, and learn information about our users' preferences.

Limitations on access to your Personal Information by employees and authorized parties:

Our employees and affiliates will not access your Personal Information without a specific reason to do so. Often this reason will be to better serve you in the event of a support issue (for example, we may look up your operating system and web browser if you write to us saying you are having a problem with the Website).

How your data is shared and transferred.

We disclose user information only as described below:

- **Student's personal information may be shared with students' schools and teachers.**
  When a student joins a class, their data, including their name, username and scores, becomes available to the teacher who created that class. This information may also be shared with other agents within the school, including other teachers and the administration.
- **Aggregated and anonymous data may be shared.**
  We will occasionally share aggregated and/or anonymized data with partners for research, evaluation, consulting or other business purposes. When this occurs, no Personal Information will be shared, however, other information, such as your city, grade level, or performance may be shared.
- **As legally required**
  In response to court orders, warrants, or subpoenas, and other situations where required by law, we may share user information. We will take reasonable steps to notify users of this sharing as soon as possible.
- **Change of business**

If we acquire, merge with, or are acquired by another organization, in whole or in part, the information we have collected may be transferred to and/or shared with the other organization and its affiliates. In such case, the organization receiving the personal information will be obligated to follow the terms of this privacy policy.

- **When appropriate or necessary to protect our interests**
  We may share information if we believe that it is reasonably necessary to enforce the Terms of Use or to protect us against liability, unlawful or fraudulent uses, or to defend ourselves against third-party allegations or claims. We may also share this information for security reasons, such as to defend the integrity of our website. Your information may also be shared to protect the personal safety, rights, or property of Quill.org, its users, and others.
- **Service providers**
  We may share information with our service providers.
- **Partners**
  We may share information about aggregated and/or anonymized data with our partners.

Your options and choices in our data use, collection, and transfer:

- **You can choose to not provide us with Personal Information**
  You may use the Website anonymously without providing any Personal Information. If you choose to do this, you will still have access to all of our lessons and content, but some Website features may not work and your progress will not be saved.
- **You can view your Personal Information**
  You can view certain personal information by logging into our website, and can request to view any other personal information by contacting us at hello@quill.org, or sending a request in writing to the address listed below.
- **Your Personal Information can be corrected, edited, or deleted**
  To ensure that you have control over your information, we will respond as quickly as possible to any request to correct, edit or delete Personal Information. If you would like this information changed or removed, please contact us at hello@quill.org, or send a request in writing to the address listed below.

Data Retention

We will retain your or your student's personal information, including after the school term in which you or your student uses the Services, for only as long as is reasonably necessary to fulfill the purpose for which the information was collected. Generally, Quill will delete a user's personal information 4 years after the user's last login to the Services.

Children Users

Children's Online Privacy Protection Act (COPPA)

To comply with COPPA, we only collect Personal Information from children under 13 after the student's school, district or teacher has agreed to obtain parental consent for that child to use our Website and to provide us with Personal Information.

While parents or guardians of children under 13 may sign up their child and provide us with Personal Information about the child, no child under 13 may sign up with us or send us Personal Information unless they are signing up through their school, district or teacher, and that school, district or teacher has obtained parental or guardian consent to use our Website and provide us with Personal Information.
If you are under 13, do not send us any Personal Information unless you are signing up through your school, district or teacher, and that school, district or teacher has obtained parental consent for you to use our Website and provide us with Personal Information.

If we find any users who are under 13 and have shared Personal Information with us without signing up through a school, district or teacher that has obtained parental consent to use our Website and provide us with Personal Information, we will delete this information as quickly as possible. If you are aware, or become aware, of any users who have violated any part of this section, please email us at hello@quill.org so that we can investigate.

If you are signing up for the Website and creating accounts on behalf of student(s), you represent and warrant that you are either (a) a teacher or school administrator or otherwise authorized by a school or district to sign up on behalf of students, or (b) the parent of such student(s). If you are a school, district, or teacher, you represent and warrant that you are solely responsible for complying with Children's Online Privacy Protection Act (COPPA) and all similar applicable laws, meaning that you must obtain advance written consent from all parents or guardians whose children under 13 will be accessing the Services. When obtaining consent, you must provide parents and guardians with this Privacy policy and our Terms of Use. You must keep all consents on file and provide them to us if we request them.

If you are a teacher, you represent and warrant that you have permission and authorization from your school and/or district to use the Services as part of your curriculum, and for purposes of COPPA compliance, you represent and warrant that you are agreeing to this Privacy policy and our Terms of Use on behalf of your school and/or district.

How we handle data security

- **Keeping your information secure**
  To protect your Personal Information, account information, and privacy, we may require you to login using a password before accessing certain parts of the Website. We urge you to create a strong password and keep this information safe.
- **We try to keep secure the Website and Personal Information within, but there are no guarantees.**
  We use a number of techniques, including technological, social and procedural methods designed to keep your information safe. These include following industry practices, working with cyber security consultants, and more. While we take reasonable steps to protect your information, we neither ensure nor warrant that information transmitted to or by us is secure, and you provide us with this information at your own risk.
- **You will be notified electronically or through the Website if there has been a security incident that may affect you.**
  If a security incident involving your Personal Information does occur, we will notify you and any other users that may have been affected as soon as possible after we learn of the security incident. This notification may occur electronically, or via a notice posted on the Website.

Links to third party sites

In some cases, the Website may link to third party websites. These links may include social media pages, partner organizations, or any other website. We cannot control the activities or content that exists on these sites, and they may change without our knowledge. This Privacy policy does not apply to those websites, or any other website that is not part of the Website.

Changes and updates to this Privacy policy

We may revise this Privacy policy from time to time. If we make any changes, we will change the last revised date listed below. The revised Privacy policy will become effective upon such posting.

If we make any material changes to this privacy, we will provide notice to the email address we have on record for each account holder. For material changes regarding use or collection of data, we will provide choices and additional information regarding the collection of such data before it is used in any manner inconsistent with the terms initially provided to users. You are responsible at all times for keeping that email address up to date.

Contacting Us

If you have any questions regarding this Privacy policy, comments, or would like to know what Personal Information has been collected about you, please contact us by emailing hello@quill.org or writing to:

Empirical Resolution Inc.
41 E 11th St
11th Floor
New York, NY 10003

Addendum B

PARENTS' BILL OF RIGHTS – SUPPLEMENTAL INFORMATION ADDENDUM

1. **EXCLUSIVE PURPOSES FOR DATA USE**: The exclusive purposes for which "student data" or "teacher or principal data" (as those terms are defined in Education Law Section 2-d and collectively referred to as the "Confidential Data") will be used by Empirical Resolution Inc. (Quill.org) (the "Contractor") are limited to the purposes authorized in the contract between the Contractor and the Wayne-Finger Lakes BOCES/EduTech (the "BOCES") dated 10/16/2023 (the "Contract").

2. **SUBCONTRACTOR OVERSIGHT DETAILS**: The Contractor will ensure that any subcontractors, or other authorized persons or entities to whom the Contractor will disclose the Confidential Data, if any, are contractually required to abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable State and Federal laws and regulations (e.g., the Family Educational Rights and Privacy Act ("FERPA"); Education Law §2-d; 8 NYCRR Part 121).

3. **CONTRACT PRACTICES**: The Contract commences and expires on the dates set forth in the Contract, unless earlier terminated or renewed pursuant to the terms of the Contract. On or before the date the Contract expires, protected data will be exported to the BOCES in **CVS** format and/or destroyed by the Contractor as directed by the BOCES.

4. **DATA ACCURACY/CORRECTION PRACTICES**: A parent or eligible student can challenge the accuracy of any "education record", as that term is defined in FERPA, stored by the BOCES in a Contractor's product and/or service by following the BOCES' procedure for requesting the amendment of education records under FERPA. Teachers and principals may be able to challenge the accuracy of APPR data stored by the BOCES in Contractor's product and/or service by following the appeal procedure in the BOCES' APPR Plan. Unless otherwise required above or by other applicable law, challenges to the accuracy of the Confidential Data shall not be permitted.

5. **SECURITY PRACTICES**: Confidential Data provided to Contractor by the BOCES will be stored in web servers in the United States. The measures that Contractor takes to protect Confidential Data will align with the NIST Cybersecurity Framework including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.

6. **ENCRYPTION PRACTICES**: The Contractor will apply encryption to the Confidential Data while in motion and at rest at least to the extent required by Education Law Section 2-d and other applicable law.

Signature: 

Date: 10/16/2023