Ref Reps

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 Ref Reps **("Vendor")** are parties to a contract dated 6/29/23 ("the underlying contract") governing the terms under which BOCES accesses, and Vendor provides, RefReps OES ("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 Ref Reps, LLC .

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 EmployeeTraining

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)
Date 7/6/23	**Date** 6/29/2023

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)**
Date 7/6/23	**Date** 6/29/2023

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)

Introduction

Thank you for visiting the RefReps Privacy Center.

The RefReps Privacy is tasked with ensuring the appropriate collection, use, sharing, and handling of your personal information. At RefReps, we take the privacy and security of your personal information seriously. We've created this Privacy Center in order to offer you the details you require around how we collect and process your personal information, no matter what your relationship is with us.

It's important to note that you may have multiple relationships with RefReps. For example, you may be both a purchaser (customer) and end-user of our products (end-user). Each notice applies to the personal information collected and processed as part of that relationship. For example, we do not use personal information collected for end-users in the same manner as we use customer information.

RefReps may, from time to time, modify any of the notices in the Privacy Center to reflect legal, technological and other developments. In that event, the changes will appear at this location and you may be notified directly as required by local law.

Contact Information

Any questions or complaints regarding this Privacy Center or RefReps' collection, use, disclosure, or transfer of personal information should be directed to the RefReps Privacy Office by emailing hype@refreps.com.

Customer

RefReps Customer Privacy Notice

Please note that this notice applies to individuals who visit RefReps commercial web sites or otherwise interact with us as customers via our web sites, social media, or at events. As a customer, you may also be an end user. Please be sure to review our End User Privacy Notice regarding our privacy practices for end user PII. Our commercial web sites, such as refreps.com, are not intended for use by minors below the age of 13. Privacy information for users of our digital learning systems, including those under the age of 13, can be found under the appropriate tabs (End User and Parents).

RefReps is a global organization. We follow privacy laws and regulations that are applicable to our company and our services in the areas where we do business. By accessing our web sites or otherwise providing your personal information to RefReps, you acknowledge that we will process your PII in accordance with this notice.

What is Personal Information?

Personally Identifiable Information, or PII, shall mean any information relating to an identified or identifiable natural person ("data subject") including personal data as defined under applicable local law. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

What Personal Information do we collect?

We collect PII, such as contact information, education details, or payment information, in order to provide you with the product and/or service requested.

We, or our service providers on our behalf, collect PII and other information when you access and/or submit PII on one of our web sites or interact with us at an event. You are not required to provide PII; however, in order to use certain services, we may need to collect certain PII for that service to function properly (e.g., to finalize your purchase) or for us to provide you with requested information.

Depending on the service or transaction, the PII we collect includes information from the following categories:

1. Name, initials or white page information: On our consumer web sites, we collect your name, initials or contact information when you create an account or purchase a product on our online store. We also collect your email address. We also collect this information if you connect with us via your social media account as an existing or potential customer.
2. Payment card industry data such as credit card number, billing address, etc.: If you make an online purchase from us, in addition to your name, we collect

payment information through a third party website, which includes billing and shipping addresses and credit card data to process your transaction.

3. Contests and Promotions: If you participate in a contest or promotion with RefReps, we collect your name, contact information, and other information necessary to enter the contest or participate in the promotion.
4. Communications: If you choose to communicate with or receive communications from RefReps via phone, text, chat, email, or any other platform for technical support, customer service, or other assistance, those interactions may be recorded and monitored to deliver the service or information requested by you.
5. Third Party Marketing Lists: RefReps also purchases and rents marketing lists from various providers including event management companies and education non-profits.

We automatically collect computer metadata and content to provide, improve, and maintain our products and services.

When you visit or make transactions on our websites, we automatically collect certain information from you through the use of cookies, web beacons or other tracking mechanisms. This includes information about your experience such as your IP address, operating systems, pages viewed, and time spent. This allows RefReps to collect information about customer usage and online behavior to tailor marketing to areas that may be more appropriate for the customer.

Third parties also collect information automatically from you across websites and over time through the use of their own cookies, web beacons, and tracking mechanisms. This information is used to enable the functions of the site, as well as customize, maintain, and improve our web sites. You may disable cookies via your browser or third party mechanisms. However, some features of our services may not function properly without them. Third parties include:

- AWS (Amazon Web Services): https://aws.amazon.com/privacy/
- Wix: https://support.wix.com/en/article/wixs-privacy-policy
- Pipedrive: https://www.pipedrive.com/en/privacy

You can change your Web browser's Internet preferences to disable or delete cookies, although that may affect certain functions on this site. To learn how to manage your cookies, please follow the instructions for your specific browser. If you wish to opt out of the use of data collected on our site to send you targeted advertising during your visits to other websites, you should adjust your browser preferences to not accept cookies. As

an alternative, the following websites will allow you to opt out of the multi-site cookies http://www.aboutads.info/choices or http://youronlinechoices.eu/.

How do we use personal information?

We will use PII to provide the requested service or to process transactions such as information requests or purchases in order to meet our contractual obligations to you.

We will also process your PII to meet our legitimate interests, for example to personalize your experience and to deliver relevant content to you; to maintain and improve our services; to generate and analyze statistics about your use of the services; and to detect, prevent, or respond to fraud, intellectual property infringement, violations of law, violations of our rights or Terms & Conditions, or other misuse of the services.

Except as described in this notice, we limit the use, collection, and disclosure of your PII to deliver the service or information requested by you. We do not collect, use, or disclose PII that is not reasonably related to the purposes described within this notice without prior notification. Your information may be combined in an aggregate and de-identified manner in order to maintain and/or improve our services.

Do we use personal information to market to you

Where we are permitted by law to do so, we will send electronic marketing communications to you as a customer, depending on your location, however you always have the option to change your marketing preferences.

Depending on your location, where legally permissible, RefReps uses your PII to provide you with materials that we believe are of interest. This includes information from the platforms on which you choose to communicate with us including email, social media accounts, mobile devices and apps, RefReps websites including text/chat functions, and your shopping cart.

In some locations, such as the European Union, we will only send electronic marketing communications to consumers if you provide your consent, however such communications may still be sent directly to businesses without consent. In all instances, you may choose to change your marketing preferences at any time by completing our Global Opt-Out Form (https://forms.gle/cXAmy1SEh2VF3EeH6), clicking

the unsubscribe button in any marketing email you receive from us, or by contacting RefReps Privacy Official (hype@gmail.com).

RefReps shares your information with third parties to provide you with marketing from us, however we will not share your PII with third parties for them to market to you on their own behalf.

Please note, whatever preferences you select for marketing, you may still receive some transactional emails related to the services or products you purchase or use.

When do we share personal information?

In general, we only share your PII in order to provide, maintain, or improve our products or services, or respond to legal requests.

1. Co-branded/Other Web Sites and Features – We share your PII with third-party business partners for the purpose of providing services to you and to manage co-sponsored events. Those business partners will be given limited access to the PII that is reasonably necessary to deliver the service, and we will require that such third parties follow the same privacy and security practices as RefReps.
2. Business Transfer – In the event of a sale, merger or acquisition, we will be able to transfer your PII to a separate entity. We will use commercially reasonable efforts to require this entity to use your PII only for authorized purposes and by authorized persons in a manner consistent with the choices customers have made under this notice, and that security, integrity, and privacy of the information is maintained.
3. Agents/Service providers – We hire other companies to perform certain business-related functions on our behalf and according to our instructions. We provide your PII to service providers that host our platform data in the cloud, for example, AWS.
4. Law Enforcement – In the event that RefReps receives a legal demand for customer data from a law enforcement agency, that request will only be honored if:
    - The request complies with all laws and clearly establishes the legal need for disclosure.
    - The request is related to a specific investigation and specific user accounts are implicated in that investigation.

- Whenever legally permissible, users shall receive notice that their information is being requested.

RefReps reserves the right to disclose to third parties non-personally identifiable information about our users and their use of the RefReps websites and related services. For example, RefReps may disclose aggregate data about the overall patterns or demographics of the users of the RefReps websites to third parties.

What rights do you have around your personal information?

You have the rights to access, export, be informed about, rectify, object to the further processing of, restrict the processing of, and withdraw consent to the processing of, and erase your PII.

1. Access and rectification: We strive to ensure that information we have about you is accurate and current. You may obtain confirmation as to whether or not PII concerning you exists, regardless of whether PII has already been recorded, and to be communicated such information in a readily understandable form. If you want to review the PII you have provided to us, or believe that the information we have about you is inaccurate, you should make a request by following the instructions below.
2. Choice & Objection to processing: With limited exceptions, you may choose to change how we use your PII at any time by following the instructions below on making a request. However, if the PII is required in order to provide you with the service or process a transaction, you may not be able to opt-out without canceling the transaction or service. You may object, in whole or in part, on legitimate grounds, to the processing of your PII, even where such processing is relevant to the purpose of the collection. In addition, you may choose whether to share information about yourself and the use of our sites with third parties such as social media sites. You can also choose whether to receive marketing messages from us (see your options in our "Do we use your PII to market to you?" section above) and you may object, in whole or in part, to such processing.
3. Restriction of processing: In specific cases (e.g., if you challenge the accuracy of the PII, while this is being checked), you can request a restriction on the processing of your PII, which can only be processed to file or defend claims.
4. Information: You may be informed a) of the source of the PII; b) of the purposes and methods of the processing; c) of the logic applied to the processing, if

processing is carried out with the help of electronic means; d) of the identity of the data controller and data processors; and e) of the entities or categories of entities to whom the PII may be communicated and who may have access to such PII in their capacity as data processor(s) or person(s) in charge of the processing.

5. Data portability: You may request that we export your PII from our systems in a readily accessible file type. If completed, this means you will have received a copy of your PII that we have retained as a result of you doing business with RefReps.
6. Withdraw consent: Where we are using your PII with your consent, you may withdraw your consent at any time, though this will not affect the lawfulness of our uses of your PII prior to the withdrawal.
7. Erasure: You may request erasure, anonymization or blocking of PII that have been processed unlawfully, including PII whose retention is unnecessary for the purposes for which it has been collected or subsequently processed, and will obtain certification to the effect that such operations, as well as their contents, have been notified to the entities to whom the data were communicated, unless this requirement proves impossible or involves a manifestly disproportionate effort. At your request, in such instances, we may therefore delete or de-identify your information. However, you should be aware that doing this may limit your use of our services. For example, if you request the deletion of your account within an ecommerce portal, you may be required to re-enter this information should you wish to make another purchase.

To exercise any of your data subject rights, you should fill in a Data Request Form (https://forms.gle/pbBXeLTMen8iB9v79) or contact RefReps Privacy Official (hype@refreps.com).

How do we protect personal information?

Our IT security team has established industry standard security measures to protect your PII from unauthorized access and use.

RefReps takes reasonable precautions to protect your information. When you submit personal information via the website, your information is protected both online and off-line. RefReps utilizes reasonable security measures to protect the security and confidentiality of your PII from unauthorized access and use.

How long do we retain personal information?

We will retain your data for the minimum amount of time necessary to accomplish the purpose for which it was collected, and thereafter no longer than is permitted under RefReps' data retention policies. We will retain and use your data as necessary to comply with our obligations, resolve disputes and enforce agreements.

For information on the retention period that applies, reach out to the Privacy Office by emailing hype@refreps.com.

Version 1.2 6/26/2023, 12:01:12 PM

End User

Introduction

As a global leader in providing digital learning systems for educators and students, RefReps is deeply committed to protecting the privacy of our end users. Whether you are using any of our Services, we collect Personally Identifiable Information that we use to provide, maintain and improve the solution. We are providing the below information so that you can understand how we protect and use your information. If you are under 18, we suggest that you review this information with your parents.

This information applies to all end users of our digital learning system. Since RefReps is a service provider to your institution, your institution Educational institutions are best able to provide you with a full understanding of their privacy practices and more information on how their end user's Personally Identifiable Information (PII) is collected, shared, and used. To obtain more detailed information about how PII is collected, used, and shared by your educational institution, please contact the appropriate individual at that institution.

In limited circumstances, end users may also be customers of RefReps and RefReps may market to them as a customer. For example, end users may purchase products or create personal accounts in our web sites. In these circumstances, they would be treated as a customer. For more information on how your data is used as a customer, please review the Customer Data Privacy Notice. By contrast, this End User Data Privacy Notice applies to end users with respect to the information collected and

processed as part of a course of instruction within the digital learning solution as determined by their educational institution or employer. Aggregated de-identified end user PII is leveraged by RefReps to improve existing or develop new educational products and services.

RefReps is a global organization. We follow privacy laws and regulations that are applicable to our company and our services in the areas where we do business. Should our privacy practices change, we will update it here, but more importantly, we will notify your educational institution in writing and obtain their consent before implementing any material impact to your privacy rights.

What is Personal Information?

Personally identifiable information, or PII, is any information relating to an identified or identifiable natural person ("data subject") including personal data as defined under applicable local law. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

What Personal Information do we collect?

We collect PII, such as contact information and education details, in order to provide you with the product and/or service requested.

We only collect the information required to provide, maintain and improve the digital learning solution you use. When you register, or are registered within one of our digital learning solutions, we collect your name, school, instructor, class, and login information. Once you begin using one of our solutions, we collect your input to questions, technical specifications, and other information about how you use the solution. You are not required to provide PII; however, in order to use certain services, we may need to collect certain PII for that service to function properly or for us to provide you with requested information.

Depending on the product, the PII we collect includes information from the following categories:

- Name, initials, and personal or business-related contact information
- For our digital learning systems, we collect your name/initials and contact information when you create an account. However, we collect additional PII, or confirm existing PII, if you contact customer service with an issue or question.
- Education & professional information
- For some digital learning systems, we collect PII related to your position as an educator or student. This includes the state, district, name of school, courses, etc.
- In some instances, we collect PII from third parties who provide single-sign-on functions via Learning Management Systems or related tools.

We automatically collect computer metadata and content to provide, improve, and maintain our products and services.

When you use our digital learning systems, we automatically collect certain information from you through the use of cookies, web beacons or other tracking mechanisms. This includes information about your experience such as your IP address, operating systems, pages viewed, and time spent.

Third parties also collect information automatically from you across websites and over time through the use of their own cookies, web beacons, and tracking mechanisms. This information is used to enable the functions of the digital learning system, as well as customize, maintain, and improve our digital learning systems. You may disable cookies via your browser or third party mechanisms. However, some features of our digital learning systems may not function properly without them. Third party cookies that we use include Google Analytics and Webtrends.

If you choose to communicate with or receive communications through our services via phone, text, chat, email, or any other platform for technical support, customer service, or other assistance, those interactions may be recorded and monitored to deliver the solution or information requested by you.

How do we use personal information?

As mentioned above, we use your information to provide you with the digital learning solution on behalf of your school, in order to meet our contractual obligation to you or your school with respect to the service. For example, to assist with identifying users

across products and providing consistent service and to enable sharing of data between our products and your school's learning management system.

We will also process your PII to meet our legitimate interests, for example to improve the quality of services and products.

Except as described in this notice, we limit the use, collection, and disclosure of your PII to the minimum level necessary to deliver the service or information requested by you or your institution. We do not collect, use, or disclose PII that is not reasonably related to a legitimate business purpose necessary to serve you. Your information may also be used in order to maintain and/or improve our services.

Some of our digital learning solutions will use your previous responses to customize your learning experience. This customization is designed to ensure the best possible learning environment for a student without directly driving any determinative outcome.

Provision of your PII may be necessary in order to use the chosen digital learning solution. Failure to provide us with your PII may preclude you from using the digital learning solution.

Do we sell end-user personal information or use it for marketing purposes?

We will not sell end user PII or use information from educational records for marketing purposes.

We will not sell PII to other organizations, nor will we market to students using the information from their educational records (education records are defined as records directly related to a student and maintained by an educational agency or institution, or by a party acting for the agency or institution).

When do we share personal information?

In general, we only share your PII in order to provide, maintain, or improve our products or services, or respond to legal requests.

1. Co-branded/Other Web Sites and Features – We may share your PII with third-party business partners for the purpose of providing the service to you. These third-party business partners include cloud service providers, learning management systems (LMS), other educational software providers, etc. These business partners will be given limited access to the PII that is reasonably necessary to deliver the service, and we will require that such third parties follow the same privacy and security practices as RefReps.
2. Business Transfer – In the event of a sale, merger or acquisition, we will be able to transfer your PII to a separate entity. We will require this entity to use your PII only for authorized purposes and by authorized persons in a manner consistent with the choices end users have made under this notice, and that security, integrity, and privacy of your PII is maintained.
3. Agents/Service providers – We hire other companies to perform certain business-related functions on our behalf and according to our instructions. For example, we provide your PII to service providers that host our platform data in the cloud (e.g., AWS).
4. Educational Institutions / Corporation – As we provide products and services to your institution / corporation, we share your data with approved individuals such as administrators or educators.
5. Law Enforcement – In the event that RefReps receives a legal demand for end user data from a law enforcement agency, that request will only be honored if:
    - The request complies with all laws and clearly establishes the legal need for disclosure.
    - The request is related to a specific investigation and specific user accounts are implicated in that investigation.
    - Whenever legally permissible, users shall receive notice that their information is being requested.

RefReps reserves the right to disclose to third parties non-personally identifiable information about our users and their use of the RefReps services. For example, RefReps may disclose aggregate data about the overall patterns or demographics of the users of the RefReps products or services.

What rights do you have around your personal information?

As an end-user, you may have the rights to access, export, be informed about, rectify, object to the further processing of, restrict the processing of, withdraw consent to the processing of, and erase your personal information.

If you are or were a student, instructor, or administrator at an educational institution using a RefReps digital product, you must direct any requests to exercise your data subject rights to the appropriate representative at your institution. Otherwise, you may reach out to RefReps directly on the requests below:

1. Access and rectification – We strive to ensure that the PII we have about you is accurate and current. You may obtain confirmation as to whether or not PII concerning you exists, regardless of whether PII has already been recorded, and be communicated such information in a readily understandable form.
2. Choice & Objection to processing – With limited exceptions, you may choose to change how we use your PII at any time. However, if the PII is required in order to provide you with the service or process a transaction, you may not be able to opt-out without canceling the transaction or service. You may object, in whole or in part, on legitimate grounds, to the processing of your PII, even where such processing is relevant to the purpose of the collection. Please know that if we do receive a request to object to the further processing of your information, you may no longer be able to access or use the digital learning solution.
3. Withdraw consent – Your educational institution is responsible for obtaining your consent, where required. RefReps obtains consent from your institution to collect, process, and store your PII.
4. Restriction of processing: In specific cases (e.g., if you challenge the accuracy of the PII, while this is being checked), you can request a restriction on the processing of your PII, which can only be processed to file or defend claims.
5. Information – You have the right to be informed a) of the source of the PII; b) of the purposes and methods of the processing; c) of the logic applied to the processing, if processing is carried out with the help of electronic means; d) of the identity of the data controller and data processors; and e) of the entities or categories of entities to whom the PII may be communicated and who may have access to such PII in their capacity as data processor(s) or person(s) in charge of the processing.
6. Data portability – You have the right to export your PII from our systems in a readily accessible file type.
7. Erasure – You may request erasure, anonymization or blocking of a) PII that have been processed unlawfully; b) PII whose retention is unnecessary for the purposes for which it has been collected or subsequently processed. You can obtain certification to the effect that such operations, as well as their contents, have been notified to the entities to whom the data were communicated, unless

this requirement proves impossible or involves a manifestly disproportionate effort. Since your educational institution has hired us to manage this information for them, we ask that you or your parent make any request to delete your information directly to your school. Please know that if we do receive a request to delete your information, you may no longer be able to access or use the digital learning solution.

How do we protect personal information?

Our IT security team has established industry standard security measures to protect your PII from unauthorized access and use.

RefReps takes reasonable precautions to protect your information. When you submit PII via the digital learning system, your information is protected both online and off-line. RefReps utilizes reasonable security measures to protect the security and confidentiality of your PII from unauthorized access and use.

How long do we retain personal information?

We will retain your data for the minimum amount of time necessary to accomplish the purpose for which it was collected, and thereafter no longer than is permitted under RefReps' data retention policies. We will retain and use your data as necessary to comply with our obligations, resolve disputes and enforce agreements.

For information on the retention period that applies, reach out to the Privacy Office by emailing hype@refreps.com.

Version 1.2 6/26/2023, 12:01:12 PM

Parent

Privacy Information for Parents

Protecting privacy and maintaining the trust of our customers, students, and their parents has always been a key priority for us. To enhance learning, we need access to data, measurement, insight and other feedback that inform us about students' knowledge, skill levels and learning development.

Our goal is to use the data obtained in the course of current learning activities to provide adaptive pathways of learning; not to drive commerce. Our commitment to privacy and innovation goes beyond compliance, it is part of our culture:

- We have implemented policies and procedures to support customers in their compliance with privacy laws, including: GDPR, COPPA, and FERPA.
- We have an internal Privacy Council comprised of senior leaders throughout our company that provides the tone at the top to perpetuate best practices across our business.
- We do not support business models that create tolls and taxes on interoperability.
- We conduct regular scans of our applications to prevent and detect security breaches. We recognize that no system is 100% secure, but we take steps to prevent and mitigate the impact of adverse events.

By increasing awareness and transparency, we hope to better understand the concerns and learn how to talk with each other about privacy, security, and confidentiality.

Educational institutions, as data controllers, are ultimately responsible for providing a full understanding of the privacy practices around how their students' personally identifiable information is collected, shared, and used. To obtain more detailed information about how data is collected, used, and shared by an educational institution, please contact the appropriate representative at that institution.

For further details on our privacy practices around student data, please review the Student Data Privacy Notice. The Student Data Privacy Notice details practices around how we collect and use student information, whether they are a student at an educational institution or an individual using a product on their own.

If you have purchased a RefReps product for your child please also review the Customer Data Privacy Notice for information on how we handle your personally identifiable information.

If you have purchased a RefReps product and created an account for yourself as an educator, please also review the Educator Data Privacy Notice. The Educator Data Privacy Notice also applies to educators at educational institutions.

If you choose to communicate with or receive communications from RefReps via phone, text, chat, email, or any other platform for technical support, customer service, or other assistance, those interactions may be recorded and monitored to deliver the information requested by you.

Version 1.2 6/26/2023, 12:01:12 PM

Student

Privacy Information for Students

Introduction

As a global leader in providing digital learning systems for educators and students, RefReps is deeply committed to protecting the privacy of our end users. Whether you are using any of our Services, we collect Personally Identifiable Information that we use to provide, maintain and improve the solution. We are providing the below information so that you can understand how we protect and use your information. If you are under 18, we suggest that you review this information with your parents.

This information applies to all students of our digital learning system. Since RefReps is a service provider to your institution, your institution Educational institutions are best able to provide you with a full understanding of their privacy practices and more information on how their end user's Personally Identifiable Information (PII) is collected, shared, and used. To obtain more detailed information about how PII is collected, used, and shared by your educational institution, please contact the appropriate individual at that institution.

In limited circumstances, students may also be customers of RefReps and RefReps may market to them as a customer. For example, students may purchase products or create personal accounts in our web sites. In these circumstances, they would be treated as a customer. For more information on how your data is used as a customer, please review the Privacy Notice. By contrast, this Student Data Privacy Notice applies to students with respect to the information collected and processed as part of a course of instruction within the digital learning solution as determined by their educational institution or employer. Aggregated de-identified student PII is leveraged by RefReps to improve existing or develop new educational products and services.

RefReps is a global organization. We follow privacy laws and regulations that are applicable to our company and our services in the areas where we do business. Should our privacy practices change, we will update it here, but more importantly, we will notify your educational institution in writing and obtain their consent before implementing any material impact to your privacy rights.

What is Personal Information?

Personally identifiable information, or PII, is any information relating to an identified or identifiable natural person ("data subject") including personal data as defined under applicable local law. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

What Personal Information do we collect?

We collect PII, such as contact information and education details, in order to provide you with the product and/or service requested.

We only collect the information required to provide, maintain and improve the digital learning solution you use. When you register, or are registered within one of our digital learning solutions, we collect your name, school, instructor, class, and login information. Once you begin using one of our solutions, we collect your input to questions, technical specifications, and other information about how you use the solution. You are not required to provide PII; however, in order to use certain services, we may need to collect certain PII for that service to function properly or for us to provide you with requested information.

Depending on the product, the PII we collect includes information from the following categories:

- Name, initials, and personal or business-related contact information

- For our digital learning systems, we collect your name/initials and contact information when you create an account. However, we collect additional PII, or confirm existing PII, if you contact customer service with an issue or question.
- Education & professional information
- For some digital learning systems, we collect PII related to your position as an educator or student. This includes the state, district, name of school, courses, etc.
- In some instances, we collect PII from third parties who provide single-sign-on functions via Learning Management Systems or related tools.

We automatically collect computer metadata and content to provide, improve, and maintain our products and services.

When you use our digital learning systems, we automatically collect certain information from you through the use of cookies, web beacons or other tracking mechanisms. This includes information about your experience such as your IP address, operating systems, pages viewed, and time spent.

Third parties also collect information automatically from you across websites and over time through the use of their own cookies, web beacons, and tracking mechanisms. This information is used to enable the functions of the digital learning system, as well as customize, maintain, and improve our digital learning systems. You may disable cookies via your browser or third party mechanisms. However, some features of our digital learning systems may not function properly without them.

If you choose to communicate with or receive communications through our services via phone, text, chat, email, or any other platform for technical support, customer service, or other assistance, those interactions may be recorded and monitored to deliver the solution or information requested by you.

How do we use personal information?

As mentioned above, we use your information to provide you with the digital learning solution on behalf of your school, in order to meet our contractual obligation to you or your school with respect to the service. For example, to assist with identifying users across products and providing consistent service and to enable sharing of data between our products and your school's learning management system.

We will also process your PII to meet our legitimate interests, for example to improve the quality of services and products.

Except as described in this notice, we limit the use, collection, and disclosure of your PII to the minimum level necessary to deliver the service or information requested by you or your institution. We do not collect, use, or disclose PII that is not reasonably related to a legitimate business purpose necessary to serve you. Your information may also be used in order to maintain and/or improve our services.

Some of our digital learning solutions will use your previous responses to customize your learning experience. This customization is designed to ensure the best possible learning environment for a student without directly driving any determinative outcome.

Provision of your PII may be necessary in order to use the chosen digital learning solution. Failure to provide us with your PII may preclude you from using the digital learning solution.

Do we sell end-user personal information or use it for marketing purposes?

We will not sell end user PII or use information from educational records for marketing purposes.

We will not sell PII to other organizations, nor will we market to students using the information from their educational records (education records are defined as records directly related to a student and maintained by an educational agency or institution, or by a party acting for the agency or institution).

When do we share personal information?

In general, we only share your PII in order to provide, maintain, or improve our products or services, or respond to legal requests.

6. Co-branded/Other Web Sites and Features – We may share your PII with third-party business partners for the purpose of providing the service to you. These third-party business partners include cloud service providers, learning management systems (LMS), other educational software providers, etc. These

business partners will be given limited access to the PII that is reasonably necessary to deliver the service, and we will require that such third parties follow the same privacy and security practices as RefReps.

7. Business Transfer – In the event of a sale, merger or acquisition, we will be able to transfer your PII to a separate entity. We will require this entity to use your PII only for authorized purposes and by authorized persons in a manner consistent with the choices end users have made under this notice, and that security, integrity, and privacy of your PII is maintained.
8. Agents/Service providers – We hire other companies to perform certain business-related functions on our behalf and according to our instructions. For example, we provide your PII to service providers that host our platform data in the cloud (e.g., AWS).
9. Educational Institutions / Corporation – As we provide products and services to your institution / corporation, we share your data with approved individuals such as administrators or educators.
10. Law Enforcement – In the event that RefReps receives a legal demand for end user data from a law enforcement agency, that request will only be honored if:
    - The request complies with all laws and clearly establishes the legal need for disclosure.
    - The request is related to a specific investigation and specific user accounts are implicated in that investigation.
    - Whenever legally permissible, users shall receive notice that their information is being requested.

RefReps reserves the right to disclose to third parties non-personally identifiable information about our users and their use of the RefReps services. For example, RefReps may disclose aggregate data about the overall patterns or demographics of the users of the RefReps products or services.

What rights do you have around your personal information?

As an end-user, you may have the rights to access, export, be informed about, rectify, object to the further processing of, restrict the processing of, withdraw consent to the processing of, and erase your personal information.

If you are or were a student, instructor, or administrator at an educational institution using a RefReps digital product, you must direct any requests to exercise your data

subject rights to the appropriate representative at your institution. Otherwise, you may reach out to RefReps directly on the requests below:

8. Access and rectification – We strive to ensure that the PII we have about you is accurate and current. You may obtain confirmation as to whether or not PII concerning you exists, regardless of whether PII has already been recorded, and be communicated such information in a readily understandable form.
9. Choice & Objection to processing – With limited exceptions, you may choose to change how we use your PII at any time. However, if the PII is required in order to provide you with the service or process a transaction, you may not be able to opt-out without canceling the transaction or service. You may object, in whole or in part, on legitimate grounds, to the processing of your PII, even where such processing is relevant to the purpose of the collection. Please know that if we do receive a request to object to the further processing of your information, you may no longer be able to access or use the digital learning solution.
10. Withdraw consent – Your educational institution is responsible for obtaining your consent, where required. RefReps obtains consent from your institution to collect, process, and store your PII.
11. Restriction of processing: In specific cases (e.g., if you challenge the accuracy of the PII, while this is being checked), you can request a restriction on the processing of your PII, which can only be processed to file or defend claims.
12. Information – You have the right to be informed a) of the source of the PII; b) of the purposes and methods of the processing; c) of the logic applied to the processing, if processing is carried out with the help of electronic means; d) of the identity of the data controller and data processors; and e) of the entities or categories of entities to whom the PII may be communicated and who may have access to such PII in their capacity as data processor(s) or person(s) in charge of the processing.
13. Data portability – You have the right to export your PII from our systems in a readily accessible file type.
14. Erasure – You may request erasure, anonymization or blocking of a) PII that have been processed unlawfully; b) PII whose retention is unnecessary for the purposes for which it has been collected or subsequently processed. You can obtain certification to the effect that such operations, as well as their contents, have been notified to the entities to whom the data were communicated, unless this requirement proves impossible or involves a manifestly disproportionate effort. Since your educational institution has hired us to manage this information for them, we ask that you or your parent make any request to delete your information directly to your school. Please know that if we do receive a request to delete your information, you may no longer be able to access or use the digital learning solution.

How do we protect personal information?

Our IT security team has established industry standard security measures to protect your PII from unauthorized access and use.

RefReps takes reasonable precautions to protect your information. When you submit PII via the digital learning system, your information is protected both online and off-line. RefReps utilizes reasonable security measures to protect the security and confidentiality of your PII from unauthorized access and use.

How long do we retain personal information?

We will retain your data for the minimum amount of time necessary to accomplish the purpose for which it was collected, and thereafter no longer than is permitted under RefReps' data retention policies. We will retain and use your data as necessary to comply with our obligations, resolve disputes and enforce agreements.

For information on the retention period that applies, reach out to the Privacy Office by emailing hype@refreps.com.

Version 1.2 6/26/2023, 12:01:12 PM