Albert.io

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 Learn by Doing **("Vendor")** are parties to a contract dated 1/30/24 ("the underlying contract") governing the terms under which BOCES accesses, and Vendor provides, Albert.io ("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 Learn by Doing.

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.

Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

Signatures

For Wayne-Finger Lakes BOCES/EduTech	**For (Vendor Name)**
	Bonnie McShane
Date 2/5/24	**Date** 1/30/24

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)**
	Bonnie McShane
Date	**Date**
2/5/24	1/30/24

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

Text

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 attach)

Attached, and you can also view it here: https://www.albert.io/privacy

Privacy Policy

Albert has been certified by iKeepSafe for compliance with FERPA and California student data privacy and security standards
Albert is compliant with Utah Student Data Privacy requirements
Last updated: 01/01/2021

1. WHAT IS ALBERT?

Albert helps students learn more effectively through engaging practice and real-time feedback. Educators use Albert to extend their instructional capacity by letting Albert challenge students with questions and providing detailed explanations that students can review at their own pace both in and out of school. Albert serves grades 5 through 12 and covers all core academic areas, including reading, writing, math, science, and social studies.

2. FORWARD AND DEFINITIONS

At Learn By Doing, Inc. ("us," "we," or "Albert"), we take the security and privacy of user data extremely seriously. We are committed to complying with the student data privacy laws that apply to your use of the Platform and helping our customers comply with FERPA, COPPA, and other regulatory requirements. Read more below and in our Terms of Use.

We use the term "User Information" in this policy to refer to information that personally identifies a user of Albert's platform as well as other information we receive or create in the course of a User's usage of the Platform that is linked to information that personally identifies a User. We use the term "Student Information" to refer to User Information that specifically pertains to Student Users of the Platform.

Capitalized words that are not defined herein have the definitions set forth in our Terms of Use.

3. DATA WE COLLECT

When you register for, and use the Platform, you may provide us with three types of User Information:

Personal Data

For the general purposes of authentication, class roster management, and compliance with applicable laws, we collect information that is used to identify individual Users (the "Personal Data"). Personal Data does not include Data that has been aggregated or made anonymous such that it can no longer be reasonably associated with a specific person.

Jiaochong Lu
Learn By Doing, Inc.

The Personal Data that we collect from Users includes:

Personal Data	User type	Purpose	Required?	Stored?
Salutation (Title)	Educators only	Identification	Yes	Yes
First and last name	Students and Educators	Identification	Yes	Yes
Email address	Students (or their Parents/Guardians) and Educators	Identification, authentication, notifications	Yes	Yes
Username	Students and Educators	Identification and authentication	Yes	Yes
Age	Students only	COPPA compliance	Yes	No
School ID code	Students only	Identification	No	Yes

As a general matter, we do not request nor collect any of the following information from Users:

- physical address(es)

Learn By Doing, Inc.

- telephone number(s
- photograph or physical likeness
- date or place of birth
- social security number
- dates of attendance in school
- grade level
- grades or test scores
- disciplinary records
- medical or health records

We collect Personal Data in different ways. For example, we collect Personal Data when Users register for an Albert account or when a teacher invites a student to join their class on the Platform by entering the student's email into the Platform and sending the student an email invitation. . We also receive Personal Data from other sources ("Integrated Services"), such as identity verification services, like Google and Clever, contingent on Users granting such Integrated Services to share Personal Data with us.

You have the right to decline to share certain elements of Personal Data that we ask you to provide, but must note that doing so may limit your use of certain features and functionality of the Platform. You may edit the Personal Data you provide to Albert at any time by accessing your account through the Platform.

Device Data

Like most web-based services, we (or our Service Providers) may automatically receive and log information from your browser or your device when you use our Platform ("Device Data"). Examples of Device Data we may automatically receive and log when you use the Platform include web browser type, IP address, your device's operating system, and your device's geolocation, among others.

Learn By Doing, Inc.

We take measures to ensure that our Platform and our Service Providers only collect the minimum amount of Device Data needed to deliver the Platform in a seamless way, help us improve our products, and deliver high-quality customer support. . The Device Data we collect is analyzed and may be aggregated and combined with similar aggregate Device Data of other users the Platform, as well as associated with the Personal Data of individual Users. If you use Albert on different devices, we may link the information we collect from those different devices to help us provide a consistent Platform experience across your different devices.

Usage Data

User interactions with our Platform generate data we refer to as "Usage Data". Usage Data for Student Users may include, for example, the lessons a student chooses to complete and how they performed on those lessons, when a student starts and stops a lesson, and student responses in the lesson. Usage Data for Educator Users may include their class rosters, the lessons they have created and assigned, and their class preferences. Usage Data will be used for educational and product development purposes only.

4. HOW WE USE DATA

Personal Data

We and our third-party software vendors ("Service Providers") use Personal Data to: (i) provide the Platform, ii) comply with applicable laws, and (iii) promote our products, systems, and tools. Examples of how we may use Personal Data include:

- To authenticate a user's identity;
- To customize the features that we make available to you;
- To respond to inquiries, send service notices and provide customer support;
- To communicate regarding a payment, and provide related customer service;
- For regulatory purposes and compliance with industry standards;
- To send communications about new features and products;
- To determine if a student is under 13 for the purposes of COPPA compliance;

Learn By Doing, Inc.

- We do not use Personal Data for maintenance, testing, or improvement of the Platform

Device Data

We use other Device Data to improve the product, deliver a consistent and enjoyable experience, debug, provide customer support, and for aggregate analysis.

Usage Data

We use Usage Data for reporting purposes to teachers and educational agencies, and to test and improve our product. We also use de-identified aggregate Usage Data to develop new products, improve or modify our Platform, conduct analysis and develop business intelligence that enable us to operate, protect, make informed decisions, and report on the performance of, our business.

Cookies and similar technologies

We and our Service Providers use cookies and local storage to help provide you with a better, faster, and safer experience. Cookies are small files that websites place on your computer as you browse the web. Local storage is an industry-standard technology that allows a website or application to store information locally on your computer or mobile device.

Here are some of the ways that we and our Service Providers use these technologies: to log you into the Platform, save your preferences, personalize your experience, and protect against abuse. You may set your browser to reject cookies; however, this may affect some functions of the Platform.

As a general matter, we consciously avoid and do not include Personal, Device and Usage Data in cookies and local storage. While we use these technologies to help identify user sessions, the information contained is only meaningful to the Platform itself.

5. HOW WE SHARE DATA

We do not disclose, share, rent, or sell any User Information to any third parties for commercial uses, such as targeted advertising. We only disclose or share User Information with bona fide Service Providers for purposes related to or arising out of the ordinary course of creation, development, operation, service, and maintenance of the Platform. Such bona fide Service Providers shall only use such User Information for such purposes and not to sell such User Information under any circumstances.

Learn By Doing, Inc.

Service Providers who do help us operate our Platform must adhere to privacy and security obligations in a manner consistent with the Company's policies and practices. Below is a list of our Service Providers with whom we may share User Information and the services they generally provide.

Service Provider	Purpose of data sharing
Appsignal	Application performance monitoring
Bugsnag	Software error monitoring
Front	Email client
Google Cloud Platform	Cloud hosting and data warehousing
Hotjar	Survey response collection and feature usage research
Customer.io	Customer messaging
Intercom	Customer support and help center

Learn By Doing, Inc.

Mode Analytics	Data science; user and product research
Pipedrive	CRM
Sendgrid	Transactional email service (e.g., password reset emails)
Slack	Internal communication
Stitch Data	Data ETL service
Stripe	Payment processing
Typeform	Survey response collection
Zapier	Web services integration

6. EDUCATOR USERS AND STUDENT INFORMATION

If you are a Student User using the Platform in connection with a teacher, school, or district (a "School"), your School administrator(s) and teacher(s) ("Educator Users" and each an "Educator User") may have the ability to access, monitor, use, edit, delete or disclose data related to Student Information. Additionally, Educator Users may create Student User accounts on behalf of students and in so doing, provide Albert with the Personal Data of students. If you are an Educator User, you agree that you will obtain and maintain all required consents from Student Users or their parents or legal guardians (when such Student Users are under the age of 13 or the age of consent in the state in which the Student resides) to allow: (i) your access,

monitoring, use, editing, deleting, and disclosure of their Student Information and our providing you with the ability to do so, and (ii) your Student Users' use of the Platform.

If a Student User enrolls in a "class" created by an Educator User on the Platform, the Student User grants permission to the Educator User to view their Personal Data and Usage Data. Enrollments are done via a unique class join code, a unique class join link, direct email invitation, or an Integrated Service.

If you are a Student User using the Platform in connection with a School and do not believe you or your parent or guardian has provided consent for the School or its Educator Users to access, monitor, use, edit, delete, or disclose data related to your Usage Data and Personal Data, please contact us immediately at hello@albert.io.

7. SECURITY

Albert secures User Information both in transit and at rest via encryption. We use modern cryptographic algorithms like AES256 with strict user access control and multi-factor authentication.

8. DATA RETENTION

We retain User Information to provide the Platform to you and our other Users and to provide a useful user experience, and not longer than is necessary to do so. When you update your User Information, we usually keep a backup copy of the prior version for a reasonable period of time in case you need to need to go back to that version.

Users may deactivate their account at any time by accessing their account through the Platform. Deactivating an account means the following:

- Users will no longer be able to access their account.

- No further activity may take place on the deactivated account.

- User accounts will no longer be publicly visible in the Platform.

- All data associated with User accounts will be kept for reporting and compliance reasons.

- User Information for Student Users up until their deactivation time will continue to be shared with any Educator User(s) and the school(s) to which they belonged.

Learn By Doing, Inc.

• School(s) that previously had access to such data will not have access following the deactivation.

A deactivated account can be restored, with all User Information intact, upon request

For Student Users who deactivate their account, except for Users (including Minor Users) who make a request for deactivation and de-identification (as discussed below), Albert will retain all of their Student Information for four years after their deactivation date. If no request for re-activation is received during that time, all Student Information will be de-identified and the account will no longer be eligible for restoration.

Following the termination of a license, a School may request that we deactivate and de-identify Student Information and we will do so, unless the School or applicable regulations require the retention of such data, in which case the records shall be de-identified upon the expiration of the retention period.

Minor Users (or their parents and/or guardians) may also request to deactivate and de-identify their accounts for any reason, including infancy, and we will do so. If you are a Minor User and would like to deactivate and de-identify your account for any reason, including infancy, please contact us at hello@albert.io.

In the case of a request for deactivation and de-identification, the following happens:

• We will obfuscate all of the Personal Data in the relevant Student User accounts. This means that their email, first name, last name, salutation, and username get replaced with a long, meaningless identifier that is randomly assigned. This is a one way change, and we can never recover the identity associated with the account after this step. We will perform this obfuscation in our database, all backups that we maintain, and in any Service Providers that we use to deliver the Platform.

• We will retain all Usage Data associated with the accounts to improve the Platform. These reasons include, but are not limited to: internal data analytics and prevention of fraud and abuse.

• This action results in the deactivation of the impacted Student User accounts, preventing them from being used or restored in the future.

• In order to request an account reactivation, please contact us at hello@albert.io. To request that Student Information be de-identified, please contact us at schools@albert.io.

Please note that the requested deletion will be as comprehensive as possible but is always subject to issues outside of our control, including applicable regulations and laws, your actions

Learn By Doing, Inc.

and the actions of third parties. We may also need to retain a copy of certain information for legal compliance purposes, including, without limitation, to avoid identity theft or fraud.

9. VIEWING AND CORRECTING INFORMATION

A parent or guardian may review Student Information in the applicable student's records by viewing the Student's Albert.io account. The Platform enables any Educator User to permit parents, legal guardians, and eligible pupils to review personally identifiable information contained in Student Information, and to correct erroneous information, in accordance with procedures established by the School.

To the extent that a User opts to share his or her profile with his or her parent or guardian, such User expressly agrees to such sharing and all related responsibilities and liabilities therewith. Minor Users or Child Users cannot opt of sharing his or her profile with his or her parent or guardian.

We fully comply with the Requirements for Accessible Electronic and Information Technology Design as laid out by the U.S. Department of Education here.

10. STUDENT DATA OWNERSHIP

Any and all student data provided to Albert, or to which Albert has been granted access, are and shall remain the sole property of the educational agency or school that provided or granted access to such records.

11. USERS UNDER 13 YEARS OF AGE

In accordance with the Children's Online Privacy Protection Act ("COPPA"), we require parental consent for students under the age of 13 who wish to use Albert ("Child Users"). Albert does not knowingly permit Child Users to register directly for our Platform without the consent of a Parent (defined below) or Educator User on behalf of a Parent. If Albert learns that Personal Data of a Child User has been collected on our Service without parental consent, then Albert will take appropriate steps to delete this information. If you are a parent or guardian ("Parent") and discover that your child under the age of 13 has an account with our Platform without your consent, please alert us at hello@albert.io.

There are two acceptable ways for Child Users to sign up for the Platform:

1 - Self registration. When a Child User registers for our Platform, we request an active class enrollment code, birthdate, username, email, password, and a parent's email address so that we can email the Child User's Parent in order to seek consent for the Child to use the Platform. Albert does not ask the Child User for any more information than is necessary to provide the

Services to the Child User or to seek parental consent. The Child User will not be able to use the Platform while request for consent from the Parent is pending. If we do not receive Parental consent within 14 days, the Child User's account will be deactivated, and their Personal Data will be deleted from our systems.

2 - School registration. When the Platform is used by a School in the classroom for an educational purpose, we permit the School to create Child User accounts and to provide the requisite consent for Albert to collect User Information of a Child User for this purpose, in lieu of parental consent. Schools may create Child User accounts using tools that we provide. When Schools create accounts in this manner, we do not request additional consent from the Parent, as we require Schools to gather those consents. Similarly, when a School or Educator User invites a Child User to join the Platform and connect to an Educator User's class using a class code, we do not require parental consent as it is the responsibility of that School or Educator User to acquire parental consent for each Child User.

Parents may provide consent for a Child User to use the Platform by responding affirmatively to an email sent by Albert to the Parent's email address provided by the Child User during account creation. If we do not receive consent from the Parent within fourteen 14) days, the Child User's account will be deactivated and the Child's Personal Data is deleted from our systems. Until a Parent provides consent in this manner, the Child User will be unable to meaningfully use the Platform.

Parents may review their child's personal information on Albert, direct us to delete it, and refuse to allow any further collection or use of their child's information by Albert by revoking their consent. Parents seeking to revoke their consent, review their child's information, and request a deletion of their child's data should contact us at schools@albert.io.

12. DATA BREACHES

Within 48 hours of learning about a data breach, or longer reasonable time as may be required by the legitimate needs of applicable law enforcement or as to take measures necessary to determine the scope of the breach and restore reasonable integrity of its systems, we will notify all Users, teachers, Parents, principals, and district administrators whose information may have been improperly disclosed, via email communication to the email address on file for each User. We will inform any Users who oversee those students (i.e. relevant teachers, Parents, principals, and district administrators) if any Student Information or Child User data is involved. This email notification will describe the nature of the data breach, the date of the breach, the types of information that were subject to the breach, and steps that are being taken to protect their Albert.io accounts going forward.

13. USER DATA RIGHTS AND DATA REQUESTS

Learn By Doing, Inc.

Certain Users may have additional personal information rights and choices based on where they live. We have tried to provide links to websites that provide more information below. If you feel that this list does not cover your rights, please alert us at hello@albert.io.

If you are a California resident, California law may provide you with additional rights regarding our use of your personal information. To learn more about your California privacy rights, visit https://oag.ca.gov/privacy.

If you are a resident of the European Union or European Economic Area, the General Data Protection Law ("GDPR") may provide you with additional rights regarding our use of your personal information. To learn more about your GDPR privacy rights, visit https://eugdpr.org/the-regulation/.

You have the right to lodge a complaint with the supervisory authority of your habitual residence, place of work or place of alleged infringement, if you consider that the processing of your personal data infringes applicable law. A list of EU data protection authorities is available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612080.

For example, certain Users (such as Users in California or the European Union/European Economic Area may have the following rights with respect to their User Information:

- The right to know what information Albert collects from you, why it is collected, and how it is shared.

- The right to have access to your User Information in a portable format, to the extent technically feasible.

- The right to have your User Information deleted by Albert and its Service Providers and to be notified when such deletion has been completed, colloquially known as the "right to be forgotten".

- The right to have incomplete or inaccurate User Information rectified and to be notified upon rectification.

- Withdraw your consent to the processing of your User Information.

- The right to request information about the categories of information that are sold and/or to opt out of the sale of personal information. (Note: what is covered as a "sale" under California law is not yet clear, but we currently do not "sell" your information, as we understand it.)

Learn By Doing, Inc.

Albert is committed to the free exercise of these rights without fear of being denied the opportunity to use the Platform. If you would like to request to review, correct, restrict or delete personal information that you have previously provided to us, object to the processing of User Information, or if you would like to request to receive an electronic copy of your User Information for purposes of transmitting it to another company (to the extent this right to data portability is provided to you by applicable law), or exercise any other rights according to applicable law, please contact us at hello@albert.io. We will respond to your request in accordance with the applicable law that governs the collection, use and deletion of your data and information. The requested deletion will be as comprehensive as possible but is always subject to issues outside of our control, including applicable regulations and laws, your actions and the actions of third parties. It is important to note that we may retain a copy of the information for archival purposes and to avoid identity theft or fraud.

14. NOTICE OF CHANGES

If we are going to make any changes to this Privacy Policy that would change our practices around what data we collect, how we collect that data, or that would lessen the previously noted protections around student data privacy in a material way, we will notify all users at least 30 calendar days in advance of making such a change. We will provide notification via the emails associated with the profiles of our users.

15. CONTACTING US

If you have any questions or comments about this Privacy Policy, please contact us at:

Privacy Director

Learn By Doing, Inc.

233 N Michigan Ave, Ste 1440

Chicago, IL 60611

hello@albert.io

(312) 470-2290

16. CALIFORNIA AB 1584 COMPLIANCE STATEMENT

Learn By Doing, Inc.

This Statement describes the policies and procedures employed by Learn By Doing, Inc. to ensure compliance with the requirements set forth in Section 49073.1 of the California Education Code (the "Code").

1. Ownership of Student Information. See Section 10 of this Privacy Policy

2. Student-generated content. The Platform does not collect or store any student-generated content. In the event the Platform is updated to incorporate such a feature, we will amend this statement to describe the means by which students may retain possession and control of student-generated content

3. Third-party access and use. See Section 5 of this Privacy Policy.

4. Parent and pupil review procedures. See Section 9 of this Privacy Policy.

5. Security and confidentiality of Student Information. Albert.io is committed to maintaining the security and confidentiality of Student Information. It has designated a Security Compliance Officer (SCO), who is responsible for: (a) ensuring that the Company's servers are protected against unauthorized access to the greatest degree possible; (b) limiting employee access to Student Information to whatever extent is required for them to perform their job functions; and (c) regularly training employees in data security procedures to further ensure compliance with company data security policies.

6. Unauthorized disclosure. See Section 12 of this Privacy Policy.

7. Post-contract data deletion. See Section 8 of this Privacy Policy.

8. FERPA compliance. Albert.io offers schools and districts utilizing the Platform the means to comply with their obligations under the Family Educational Rights and Privacy Act (20 USC §1232(g)), by enabling Educator Users to inspect and review Student Information and to correct any inaccuracies therein as described in Section 8 of this Statement.

9. Prohibition against targeted advertising. See Section 5 of this Privacy Policy.

17. INTERNATIONAL PRIVACY PRACTICES

If you are using the Platform, including the Site outside of the United States, your data and information is collected in the country in which you are located and is transferred to the United States or another country where our servers are located.

Learn By Doing, Inc.

18. CHANGE OF CONTROL

Over time, Albert may grow and reorganize. We may share your User Information with affiliates such as a parent company, subsidiaries, joint venture partners or other companies that we control or that are under common control with us, in which case we will require those companies to agree to use your User Information in a way that is consistent with this Privacy Policy.

In the event of a change to our organizations such that all or a portion of Albert or its assets are acquired by or merged with a third-party, or in any other situation where User Information that we have collected would be one of the assets transferred to or acquired by that third-party, this Privacy Policy will continue to apply to your User Information, and any acquirer would only be able to handle your User Information as per this policy (unless you give consent to a new policy). If you do not consent to the use of your Personal Data by such a successor company, subject to applicable law, you may request its deletion from the company.

In the unlikely event that Albert goes out of business, or files for bankruptcy, we will protect your Personal Data, and will not sell it to any third-party.

Learn By Doing, Inc.