Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

EDUTECH

Edlio

CONTRACT ADDENDUM

Protection of Student Personally Identifiable Information

1. Applicability of This Addendum

The Wayne-Finger Lakes BOCES/EduTech) and Edlio, LLC **("Vendor")** are parties to a contract dated 09/26/2023 ("the underlying contract") governing the terms under which BOCES accesses, and Vendor provides, Edlio CMS ("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 Edlio, 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 Employee Training

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

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

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

7. Ownership and Location of Protected Information

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

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

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

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

8. Purpose for Sharing Protected Information

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

9. Downstream Protections

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

10. Protected Information and Contract Termination

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

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

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

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

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

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

11. Data Subject Request to Amend Protected Information

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

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

12. Vendor Data Security and Privacy Plan

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

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

12.3. align with the NIST Cybersecurity Framework 1.0;

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

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

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

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

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

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

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

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

13. Additional VendorResponsibilities

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

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

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

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

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

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

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

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

Signatures

For Wayne-Finger Lakes BOCES/EduTech	For (Vendor Name)
	Sara Cannon
Date	**Date**
9/27/23	09/26/2023

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)
	Sara Cannon
Date	**Date**
9/27/23	09/26/2023

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)

Addendum B

PARENTS' BILL OF RIGHTS – SUPPLEMENTAL INFORMATION ADDENDUM

1. **EXCLUSIVE PURPOSES FOR DATA USE**: The exclusive purposes for which "student data" or "teacher or principal data" (as those terms are defined in Education Law Section 2-d and collectively referred to as the "Confidential Data") will be used by [Edlio, LLC.] (the "Contractor") are limited to the purposes authorized in the contract between the Contractor and the Wayne-Finger Lakes BOCES/EduTech (the "BOCES") dated **[insert contract date]** (the "Contract").

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

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

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

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

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

Privacy Policy

Last updated August 11, 2023

Edlio, LLC ("Edlio") provides this Privacy Policy to inform you of our policies and procedures regarding the collection, use and disclosure of Personally Identifiable Information we receive when you use Edlio applications. If you have questions or concerns regarding this Privacy Policy, you should first contact Edlio at info@edlio.com.

This Privacy Policy may be updated from time to time to reflect new technology, your needs, and business developments. We will notify you of any material changes by posting the new Privacy Policy on the Application. You are advised to consult this Privacy Policy regularly for any changes.

1. Our Policy Towards Children.

The Children's Online Privacy and Protection Act ("COPPA") requires that online service providers obtain parental consent, with limited exceptions, before they knowingly collect personally identifiable information online from children who are under 13. Edlio does not knowingly collect or solicit personally identifiable information from a child under 13, except for that child's name, email address, and the parent or guardian email address, which is the limited amount of personally identifiable information we are allowed to collect in order to provide notice to parents regarding the fact that we may contact their child multiple times for the purpose of providing the service that their teacher has signed up for. If we learn we have collected personal information from a student under 13, except for that child's name, email address, and child's parent's email address, without parental consent being obtained from his or her parent or guardian, or if we learn a student under 13 has provided us personal information beyond what we request from him or her, we will delete that information as quickly as possible. If you believe that a student under 13 may have provided us personal information in violation of this paragraph, please contact us at info@edlio.com .

References to "Personal Information" in this Privacy Policy shall apply to personal information of individual users of the Application.

2. Definitions.

Before you review this Privacy Policy, we recommend you are familiar with the following concepts and terms so that you can best understand how Edlio uses data about you and to enhance your experience using the Application.

2.1 We.

"We" is defined as "Edlio, LLC".

2.2 API.

An application programming interface or "API" is a particular set of rules and specifications that allows one software program to access and make use of another software program. It helps facilitate the interaction between applications, similar to the way the user interface facilitates interaction between humans and computers. Edlio uses APIs to enable programming or other similar third-party technologies, products, or activities available through the Application.

2.3 Cookies and other Tracking Technologies.

Cookies are small text files that web servers typically send to users' computer when they visit a website. Cookies can be used on mobile applications as well. Cookies can be read or edited when the user loads a website or advertisement from the domain that wrote the cookie in the first place. Cookies are used by companies to collect and send information about a user's visit – for example, number of visits to the application, average time spent, pages viewed, navigation history through the website, and other statistics. This information can be used to improve a user's online experience by saving passwords, or allowing companies to track and improve website loading times, for instance. Cookies can also be used to track a user's browsing or online purchasing habits and to target advertisements to specific users. Cookies cannot be used to access any other data on a user's mobile device, to personally identify them, or to act like malware or a virus. Users who prefer not to accept cookies on the web can set their Internet browser to notify them when they receive a cookie or to prevent cookies from being placed on their hard drive. You can read more about cookies at http://www.allaboutcookies.org/cookies/. We may also use "pixel tags," "web beacons," "clear GIFs" or similar means (individually or collectively "Pixel Tags") in connection with our Application to collect usage, demographic and geographical location data. A Pixel Tag is an electronic image, often a single pixel that is ordinarily not visible to users and may be associated with cookies on a user's hard drive. Pixel Tags allow us to count users who have visited certain screens of the Application, to deliver branded Application and to help determine the effectiveness of promotional or advertising campaigns.

2.4 Personally Identifiable Information.

We define personally identifiable information (or "PII") as "information that can be used to uniquely identify, contact, or locate a single person or can be

used with other sources to uniquely identify a single individual." e. g. name, address, social security number, e-mail address etc. This is the common industry definition used by most Internet companies. Information that call "non-PII."

Certain Non-Personally Identifiable Information would be considered a part of your Personally Identifiable Information if it were combined with other identifiers (for example, combining your zip code with your street address) in a way that enables you to be identified. However, the same pieces of information are considered Non-Personally Identifiable Information when they are taken alone or combined only with other Non-Personally Identifiable Information (for example, your viewing preferences).

3. Information Collection and Use.

Our primary goals in collecting information are to provide and improve our applications, including communication features and capabilities, to administer your account, and to enable users to enjoy and easily navigate the applications.

3.1 What We Collect.

1. Personally Identifiable Information.
    1. In the course of using the applications, we will ask you to provide us with certain Personally Identifiable Information that can be used to contact or identify you and administer your account. Personally Identifiable Information includes, but is not limited to, your name, mobile number, e-mail address, school affiliate and or student affiliation, if applicable.

1. Required Account information.
    1. Please be aware that when you register with Edlio and set up an account (each a "User"), you will at minimum have to download the Application onto your mobile device.
    2. We may track your mobile device using an identifier ("User ID") assigned by Edlio. This is a number different from your unique mobile device identification (such as "UDID") or phone number.
    3. No other information is required to participate; however you may choose to provide additional information such as personal or corporate email addresses, photographs, and other contact information.

1. Information regarding your use of the Application.
    1. Our Application also automatically collects log data about your use of the Application, for example, how you communicate with teachers, guardians, administrators, which features you use most, when you are active on the Application, when you have read communications sent through the Application, and what device you are using.

3.2 Why We Collect Your Information and How We Use It.

1. Primary Use.
   We use your Personally Identifiable Information (in some cases, in conjunction with your Non-Personally Identifiable Information) mainly as follows:
    1. to administer your requests;
    2. as part of our efforts to keep the Application and integrations safe and secure;
    3. to protect Edlio's or User content rights or property;
    4. for internal operations, including troubleshooting, data analysis, testing, research and Application improvement.

1. Combined Data.
   We may combine your Personally Identifiable Information with Non-Personally Identifiable Information and aggregate it with information collected from other Users to attempt to provide you with a better experience, to improve the quality of the Application and to analyze and understand how our Application are used. We may also use the combined information without aggregating it to serve you specifically, for instance to deliver a product to you according to your preferences or restrictions.

1. Notifications.
   We also use your Personally Identifiable Information to contact you with marketing or promotional materials and other information about the Application that may be of interest to you. If you decide at any time that you no longer wish to receive such communications from us, please follow the unsubscribe instructions provided in any of the communications. We will endeavor to comply with your request as

soon as reasonably practicable. Please note that if you opt-out as described above, we will not be able to remove your Personally Identifiable Information from our databases or those of our third party service providers to which we have already provided your Personally Identifiable Information as of the date that we implement your opt-out request. Edlio does not share, sell, rent or trade your Personally Identifiable Information with third parties for such third party's direct marketing purposes.

3.3 What We Share.

1. Your Contacts on the Application.
   By using the Application, users that you have connected with through the Application such as Teachers, Guardians, or Admins will have access to the following information about you:
   1. Knowledge that you use the Application when they join.
   2. Your profile picture.
   3. Whether you've volunteered for an event.
2. Permissible Use.
   While you are allowing us to use the information we receive about you, you always own all of your information. Your trust is important to us, which is why we don't share information we receive about you with others unless we have:
   1. received your permission;
   2. given you notice, such as by telling you about it in this policy; or
   3. removed your name or any other personally identifying information from it.
3. Third Party Services That You Access.
   Of course, for information others share about you, they control how it is shared. Please note that third parties sites and applications that you access from the Application may use cookies and track your information as well. When using third party services, we suggest you familiarize yourself with their privacy policies and terms and conditions.
4. Your Contacts on the Application.
   By using the Application, users that you have connected with through the Application such as Teachers, Guardians, or Admins will have access to the following information about you:
   1. Knowledge that you use the Application when they join.
   2. Your profile picture.
   3. Whether you've volunteered for an event.

1. Other.
   We may make your personally identifiable information available to other companies, applications or people. For example we may share:
   1. Information you choose to provide in the course of your use of the Application by communicating it to other users of the Application, by being associated with an event, a child's class or activity group communications.
   2. Information you allow us to share when you register with us, or through a subsequent affirmative election.or
   3. Information used when and if we hire or partner with third parties to provide specialized services on our behalf, such as credit card processing, data processing, customer/support services and other products or services that we choose to make available to our Users.
   4. We may share your information with a third party when we jointly offer a service or a feature with that third party, such as connectivity with other websites or applications, to provide personalization to the Application.
   5. We may share your information in order to (i) protect or defend the legal rights or property of Edlio our business partners, employees, agents and contractors (including enforcement of our agreements); (ii) protect the safety and security of Edlio users or members of the public including acting in urgent circumstances; (iii) protect against fraud or risk management purposes; or (iv) comply with the law or legal process.
   6. We also may use and share non-personally identifiable information, such as general demographic or location information, or information about the mobile device or desktop from which you access the Application. Additionally, we may de-identify personally identifiable information and share it in a de-identified or aggregated form with third parties, advertisers and/or business partners in order to analyze Application usage, improve the Application and User experience, or for other similar purposes. The use and disclosure of such information is not subject to any restrictions under this Privacy Policy.

4. Notifications and Other Messages.

We may send you notifications and other messages using the contact information we have for you, like your operating system.

If we make changes to this Privacy Policy we will notify you by publication here.

If the changes are material, we will provide you additional, prominent notice as appropriate under the circumstances.

5. Change of Control.

If the ownership of our business changes, we may transfer your information to the new owner so they can continue to operate the Application. But they will still have to honor the commitments we have made in this Data Use Policy.

6. Aggregate Information and Non-Personally Identifiable Information.

We may share aggregated information that does not include Personally Identifiable Information and we may otherwise disclose Non-Personally Identifiable Information and Log Data with third parties for industry analysis, demographic profiling and other purposes. Any aggregated information shared in these contexts will not contain your Personally Identifiable Information.

7. Service Providers.

We may employ third party companies and individuals to facilitate the Application available therein, to provide the Application on our behalf and to perform Application related to administration of the Application ("Service Providers"). The types of Service Providers we use include, without limitation, Application providers that provide the following types of Application: website and application maintenance, hosting, database management, data analytics and administration. These third parties have access to your Personally Identifiable Information only to perform these tasks on our behalf and are obligated not to disclose or use it for any other purpose.

8. Compliance with Laws and Law Enforcement.

Edlio cooperates with government and law enforcement officials and private parties to enforce and comply with the law. We will disclose any information about you to government or law enforcement officials or private parties as we, in our sole discretion, believe necessary or appropriate to respond to claims and legal process (including but not limited to subpoenas), to protect the property and rights of Edlio or a third party, to protect the safety of the public or any person, or to prevent or stop any activity we may consider to be, or to pose a risk of being, illegal, unethical, inappropriate the foregoing.

9. Deleting and Deactivating your Account.

All Users may delete their account. If you choose to delete your account, Edlio may retain an archive copy of your account information for up to one (1) week after which the content will be fully purged. Edlio will only retain archive copy for longer than one (1) week if required by law or for legitimate business purposes. Users may delete their accounts by uninstalling the Application. Edlio may retain an archived copy of your records as required by law or for legitimate business purposes.

10. Security.

Edlio is very concerned with safeguarding your information. We are not in the business of providing information security. We use our best commercial efforts to employ limited data security measures, such as encryption, on some but not all systems. No method of transmission over the Internet, or method of electronic storage, is 100% secure, however. Therefore, while Edlio strives to use commercially acceptable means to protect your Personally Identifiable Information, Edlio cannot guarantee its absolute security. Do not provide your Personally Identifiable Information if you are concerned with its disclosure. We do our best to keep your information secure. We try to keep the Application available, bug-free and safe, but do not make guarantees about any part of our Application.

We will make any legally required disclosures of any breach of the security, confidentiality, or integrity of your unencrypted electronically stored "personal data" (as defined in applicable state statutes on security breach notification) to you via e-mail or conspicuous posting via the applications in the most expedient time possible and without unreasonable delay, insofar as consistent with (i) the legitimate needs of law enforcement or (ii) any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

We store data for as long as it is necessary to provide the applications to you and others, including those described above. Typically, information associated with your account will be kept until your account is deleted. For certain categories of data, we may also tell you about specific data retention practices.

11. International Transfer.

Your information may be transferred to - and maintained on - computers located outside of your state, province, country or other governmental jurisdiction where the privacy laws may not be as protective as those in your jurisdiction. Your consent to this Privacy Policy followed by your submission of

such information represents your agreement to transfer of data across servers located in various states and countries.

12. Phishing.

Identity theft and the practice currently known as "phishing" are of great concern to Edlio. Safeguarding information to help protect you from identity theft is a top priority. We do not and will not, at any time, request your credit card information or national identification numbers in a non-secure or unsolicited e-mail or telephone communication. For more information about phishing, visit the Federal Trade Commission's website.

13. Your California Privacy Rights.

California law permits residents of California to request certain details about what Personally Identifiable Information a company shares with third parties for the third parties' direct marketing purposes. Edlio does not share your information with third parties for the third parties' own and independent direct marketing purposes unless we receive your permission. If you have questions about our sharing practices or your rights under California law, please write us at info@edlio.com.

14. Contacting Edlio.

If you have any questions about the Privacy Policy, please contact Edlio at info@edlio.com.