Budget Challenge



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 Budget Challenge **("Vendor")** are parties to a contract dated 3/29/2023 ("the underlying contract") governing the terms under which BOCES accesses, and Vendor provides, Budget Challenge ("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 ProperLiving, LLC , dba Budget Challenge

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 anyparty.

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) |
|---|---|
| | DocuSigned by: David Buten<br>20EDBEEDD94F455... |
| Date 4/4/23 | Date 3/29/2023 |

David Buten
Co-Founder/Co-CEO

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) |
|---|---|
| | DocuSigned by: David Buten 20EDBEEDD94F455... David Buten Co-Founder/Co-CEO |
| Date 4/4/23 | Date 3/29/2023 |


Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

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

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

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

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

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

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

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

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

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

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

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

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

**Notification Requirements**
**Methods of Notification**

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

a) Written notice;

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

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

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

**Data Protection Officer**

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

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

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

**Annual Data Privacy and Security Training**

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

**References:**

Education Law §2-d

8 NYCRR §121

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

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

**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)

Budget Challenge - Privacy Policy - (https://www.budgetchallenge.com/Privacy.aspx)

This Privacy Policy ("Policy"), effective October 21st, 2022, tells you about ProperLiving's (dba Budget Challenge) privacy practices governing personal information we may collect when you visit our budgetchallenge.com website (including any subdomains and mobile apps), and how we may use and share that information. Your prior activities on the site may have been governed by an earlier version of this Policy.

From time to time, we may use your information for new, unanticipated uses not previously disclosed in our Policy. If our information practices do change materially, we will post the changes to our website and revise our Policy accordingly. In addition, if we have collected personally-identifying information from you, we will notify you and secure your consent before using your personal information in new ways.

Special Note about Children's Information: Programs, games, contests, and services offered through budgetchallenge.com and any related subdomains are not marketed to children under the age of 13, nor do we knowingly collect information, or permit schools to collect information on our behalf, from children under the age of 13.

Special Note about Parent's Bill of Rights: To protect students participating in the Budget Challenge, we do not collect Personal Information. We cannot identify you in our system, and we cannot confirm parent-student relationships. For this reason, some elements of the Parents Bill of Rights are simply inapplicable to our site. Parents/legal guardians should direct any request for student records, correction or updating of student information, and/or transfer of student-generated content to personal accounts to the student's teacher or school.

Special Note about Data Ownership: We do not accept student data from the schools. Therefore, any provisions relating to ownership or processing of such data outlined in student data privacy agreements that are predicated on the schools providing student data do not apply.

What Information Do We Collect? (See also the section below on our Budget Challenge Bill-Pay Companion App.)

Personal Information:

We collect personal and contact information you choose to provide to us in connection with your activities on the site. What we collect depends on whether you are a teacher or student, and how your school wants you to interact with the site

TEACHERS:

To register for Budget Challenge, you will be asked for your first and last name, school name and school address, phone number and email address. You will also set up a username and password. You will also be asked to provide a class team name for identification of the class on publicly visible webpages. You have full discretion on whether to choose a name that may reveal identifiable information (such as school name, city, mascot, state, teacher, etc.) or not.

STUDENTS:

To register for Budget Challenge, your teacher will provide you with the class code, which you will use to create your individual account. We will match that up with your school name and address which has already been provided to us when your teacher registered the class. You will also set up a username and password. In addition, if you submit questions to the site during the simulation, we collect any information you provide in asking your question. When you create your username and password, and later if you submit any questions during the simulation, please do not include any personally identifying information. All usernames and passwords should be completely unrelated to your personal identity, and you should not disclose your identity in any questions you submit. If you are not sure whether information is personally identifying, check with your teacher.

You will be asked to provide answers to a few security questions to facilitate password reset in the event you are unable to remember your password. These questions are not designed to collect information that could be used to identify you.

In some cases, where approved by the school, students will provide email addresses as well. These email addresses are not permitted to contain personally identifiable information such as your first and/or last name or initials. If you are not sure whether your email address is personally identifying, check with your teacher.

Other user information we collect:

In addition, for each visitor to our site, we automatically gather certain other potentially identifying information and store it in log files. This information includes (as applicable) internet protocol (IP) addresses and last login date and time. We collect and store this information on an individual basis and in aggregate, or combined, form. We use proprietary algorithms to calculate various behavior, knowledge, and skill statistics using individual simulation activity for each student. We also collect both user-specific and aggregate information on what pages visitors access or visit.

"Do Not Track" Signals. We do not currently have the capability to recognize browser "Do Not Track" signals. We adhere to the standards set forth in this privacy policy.

Cookies – A cookie is a small text file that is stored on a user's computer for recordkeeping purposes. If you reject cookies, you may still use our site, but your ability to use some areas of our site will be limited. We use session cookies to make it easier for you to navigate our site. We use session cookies to record session information, such as which web pages a user has visited, and to track user activity on the site. We use session cookies to store a unique one-time use authentication token assigned to your session. This value is encrypted and does not contain any personally identifying information. These cookies expire once the session is terminated either because the user has logged out or the user's browser is closed.

Analytics – To determine how many users visit our site, how often they visit this site, and to better understand the areas of greatest interest to our visitors, we use tools called "Google Analytics" to compile this information for us. As a result of your visit to our site, these companies may collect information such as your domain type, your IP address and clickstream information. We do not combine the information collected through the use of analytics tools with personally identifiable information. For more information about the analytics companies' ability to use and share information about your visits to this site, see http://www.google.com/intl/en/policies/privacy/

Ad Networks – We do not use ad networks on our site, and we do not host ads for others.

How Do We Use and Share the Information We Collect?

We store and process teachers' Personal Information to facilitate registration of classes and participation in, and/or observation of, the Budget Challenge simulations. We may also use teacher contact information to notify teachers of other programs we think would be of interest; teachers may unsubscribe from such email messages at any time. We also use teacher emails to facilitate password reset in the event you are unable to remember your password.

We use information we collect to analyze trends, to administer the site, and to track users' movements around the site. We also use this information to improve the simulations and to make our site more useful to visitors.

School administrators may be provided reports that reflect summary statistics of students and individual teachers upon request.

The following Personal Information you provide to us through the site is displayed to others as follows:

TEACHERS: Your name, school, school state, and class averages will be added to our list of winning teachers if your class wins a simulation by achieving the highest class average score. All class team names, class score average, and class engagement average may be visible to the public on a leaderboard per simulation.

STUDENTS: You have agreed not to provide any Personal Information through the site.

We do not share Personal Information we collect with any third parties, except as follows:

If you are a student participating in a sponsored contest within Budget Challenge, we do not have your Personal Information, but your teacher will share your contact information with the sponsor if you are deemed the winner of any prize.
We share information to the extent reasonably necessary to comply with law enforcement requests and judicial proceedings, and to ensure the safety and security of the site.
We may engage in research with academic institutions. However, if we do so, we will use only non-personally-identifiable data sets.
It is possible that, at some time in the future, our company may be sold along with its assets, or may engage in business transactions in which customer information is one of the assets transferred. In such a case, the customer information which we have gathered may be one of the business assets we transfer.

How Long Do We Keep the Information We Collect?

TEACHERS: We will retain your contact information after the end of a simulation so that you do not have to re-register with each group of students participating, and so that we may contact you with other programs of interest. If, at any time after the simulation, you wish to have your contact information deleted, please let us know.

STUDENTS: We will retain student username and password information, which do not contain Personal Information, indefinitely. We will also automatically delete any email addresses 60 days after the end of your participation in a Budget Challenge simulation.

We will retain nonidentifying information indefinitely to improve the Budget Challenge simulations.

Budget Challenge Bill-Pay Companion App

As part of the Budget Challenge simulation, students have the opportunity to pay bills, review bills, and request support through the Bill-Pay Companion App downloaded to the student's phone. Teachers may also access the App, but there is no teacher-specific functionality. Your login credentials will be the same ones you use for the site; no additional personal information is requested prior to or during use of the App. Only users who have accounts on the site can access the App; the App is not an entry point to the simulation. When you use the App, we will collect your phone's UDID (unique device identifier). The UDID will be stored only if you opt into push notifications when launching the App. We do not access any other information on your phone.

How to Correct Information

Teachers may request updates or corrections to your Personal Information that we maintain. Send your request to the postal address or email address provided below. To help us process your request, please provide sufficient information to allow us to identify you in our records.
We reserve the right to ask for information verifying your identity prior to updating or correcting any information for you, or deleting your information. Should we ask for verification, the information you provide to verify your identity will be used only for that purpose, and all copies of this information in our possession will be destroyed when the process is complete.

Security

The security of your Personal Information is important to us. We follow generally accepted industry standards to protect the personal information submitted to us, and to guard that information against loss, misuse, or alteration.
Please note, however, that no method of transmission over the internet, or method of electronic storage, is 100% secure. Therefore, while we use commercially-reasonable means to protect your personal information, we cannot guarantee its absolute security.

Links to Third Party Sites

This Policy applies only to information collected by this website. From time to time, this website may link you to other sites ("Linked Sites") that are not owned by us. We do not control the collection or use of any information, including Personal Information, that occurs during your visit to the Linked Sites. Further, we make no representations about the privacy policies or practices of the Linked Sites, and we are not responsible for their privacy practices.
Be careful of disclosing any of your personally identifiable information when leaving our site. We encourage you to be aware when you leave our site and to read the privacy statements of every website that collects personally identifiable information.

Questions About Our Privacy Policy and Practices

If you have any questions about the Policy or our privacy practices, you may contact:
ProperLiving, LLC
3874 Paxton Ave., #9115
Cincinnati, Ohio 45209
513-335-0619
support@budgetchallenge.com