Xtra Math

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 XtraMath **("Vendor")** are parties to a contract dated 02/16/2024 ("the underlying contract") governing the terms under which BOCES accesses, and Vendor provides, XtraMath ("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 XtraMath.

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 or expires.

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

Date 2/20/24

For (Vendor Name) XtraMath

Roy King

Date 02/16/2024

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) XtraMath
[signature]	Roy King
Date 2/20/24	**Date** 02/16/2024

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 attach)

XtraMath Privacy Policy

Introduction

XtraMath is a not-for-profit, 501(c)3 organization, committed to protecting everyone's data privacy. This is our current Privacy Policy, which explains what user data we collect and how we use it. This policy and our Terms of Service are known collectively as our "Terms." We may change these Terms from time to time, but will provide notice as specified in the Terms of Service document.

Summary

- We collect the minimum amount of data required to operate our program.
- We use parents' and teachers' Personal Data to operate our program and, with their permission, to contact them about the program.
- We use students' Personal Data only to operate our program.
- We use de-identified student data to improve our program.
- We protect student data and have signed the Student Privacy Pledge.
- We do not advertise to students, and will not sell or rent their data in any way.
- We comply with applicable data privacy laws, such as FERPA, COPPA, CCPA, and GDPR.
- We never sell user data to third parties.

What data we collect

XtraMath collects the minimum amount of data required to operate our program. Below we summarize the data we collect on students, teachers, and parents. For an up-to-date list that shows what user data we collect, and how we use that data, see Appendix B, Record of Data Processing.

DEFINITIONS

- **Data** includes all information connected with a person's or educational entity's use of XtraMath. This includes, but is not limited to, Personal Data, metadata, usage and performance data.
- **Personal Data** includes any data that can directly or indirectly identify an individual person. For example: an email address is always considered Personal Data; a student's grade level generally is not, but could be in conjunction with other information.
- **School** includes: individual schools; teachers acting on behalf of schools; school districts; and other local educational entities.

STUDENT DATA

We collect a student's first name, grade level, and program settings from the student's parent or teacher. As the student uses XtraMath, we collect usage and performance data, such as when they signed in, how many questions they answered correctly, and how long it took them to answer questions. If a student signs in via a single sign-on provider, such as Google, we collect an identifier from the provider that allows us to authenticate their sign-in. We do **not** collect the student email address that may be used for such a sign-in.

Other personal information about the student could be inferred from data that we collect. If a student account belongs to a class, for example, then we could infer that they attend a certain school.

PARENT DATA

We collect a parent's name and email address when they sign up for an account. If they sign up using a single sign-on provider, we also collect an identifier that allows us to authenticate their sign-in. We also collect some metadata and account settings, such as their time zone, the language they used to sign up, and their email preferences.

A parent supplies a password when they create an account. The password is hashed (scrambled) on the user's computer before it is ever sent to XtraMath. We do not have access to a user's original password, and cannot obtain it from the hashed version that we receive.

Other personal information about the parent could be inferred from data that we

collect. For example, we could infer that a parent whose account is linked to a student account is the parent or guardian of that student.

TEACHER DATA

We collect the same data for teacher accounts as parent accounts, with a few additions. For example, we collect the name by which students address the teacher, such as "Ms. Smith." We also collect information about each class that the teacher creates, such as its name and its end date.

Other personal information about the teacher could be inferred from data we collect. For example, we could infer that the teacher works at a specific school based on their email address.

How We Use and Share Data

XtraMath processes user data in order to establish and maintain accounts, to provide educational activities to students, to compile and deliver reports about those activities to teachers and parents, and to understand and improve our program's effectiveness. For an up-to-date list that shows the specific types of user data we collect, and how we use that data, see Appendix B, Record of Data Processing.

STUDENT DATA

A student's Personal Data is used internally to provide the student with appropriate educational activities, and to report their performance to their parents and teachers. We may access student Personal Data when providing customer support or investigating a reported issue with our program.

PARENT AND TEACHER DATA

A parent's or teacher's Personal Data is used internally for sign-in purposes and, with permission, to send them reports, announcements, and alerts related to XtraMath. We may access a parent's or teacher's Personal Data when providing them with requested support.

PARENT AND TEACHER DATA

We release Personal Data to third parties only in the following circumstances:

- *When the user requests the disclosure*, such as a teacher sharing their class with another teacher.
- *When the third party is a trusted service provider, and the data is required to adequately perform the service. We carefully vet our service providers and their security practices. For details, see Appendix A, List of Third Party Providers.*
- *When required by law or a court order.*
- *In the event of a joint venture, sale or merger with a third party. The third party would be required to uphold our Terms, including our Privacy Policy for all existing accounts. We would provide advance notice before sharing data with that third party.*

XtraMath never releases Personal Data for any kind of third-party advertising.

USE OF DE-IDENTIFIED DATA

We may use de-identified usage data internally to analyze and improve our educational services, and to develop new products or features. We will never attempt to re-identify data that has been de-identified.

We may release de-identified data to educational researchers for the purpose of evaluating the effectiveness of our program.

We will not release de-identified data unless we are confident it cannot be re-identified, due to the removal of all direct and indirect personal identifiers, and the educational researchers have agreed in writing that they will not attempt to re-identify any individuals, classes, or Schools.

We may use aggregate de-identified data, such as the number of users of our service, for promotional purposes.

How We Securely Store Data

XtraMath takes security seriously. We implement a variety of industry-standard security measures to prevent any unauthorized access to our users' data. Such measures include, but are not limited to: data minimization; encrypting data in transit via HTTPS; hashing sensitive data, like passwords; deletion of outdated data; locked physical facilities; employee training; and administrator account security.

DATA STORAGE AND INTERNATIONAL TRANSFER

XtraMath stores and processes all data on servers in the United States. All servers that store XtraMath data are operated by trusted third party processors with whom we have contractual Data Processing Addendums. Our providers are certified under the EU-US Privacy Shield and Swiss-US Privacy Shield, to better protect the data of our international users. For details, see Appendix A, List of Third Party Providers.

DATA BREACH RESPONSE

While we use industry-standard practices to safeguard data, no service can guarantee absolute data security. We have a Breach Response Plan, which we will follow if we ever discover that Personal Data has been accessed improperly. As part of our response, we will: take action to stop further data loss or unauthorized access; investigate how the breach occurred; promptly contact all affected users via email; and contact law enforcement and government agencies when appropriate.

Data Retention and Deletion

XtraMath retains Personal Data only for as long as necessary to ensure continuity of math skill-building for students, and for the convenience of parents and teachers. We close user accounts, and delete all associated identifiable data, upon request. Most types of data are also deleted automatically after a certain amount of time has passed. For details, see Appendix B, Record of Data Processing.

We may retain de-identified, aggregate data, which cannot identify any individual user, for research and program improvement purposes. Such data is deleted once no longer necessary for these purposes.We will provide certification of data deletion upon request.

DATA BREACH RESPONSE

Compliance with Data Privacy Laws

While we use industry-standard practices to safeguard data, no service can guarantee absolute data security. We have a Breach Response Plan, which we will follow if we ever discover that Personal Data has been accessed improperly. As part of our response, we will: take action to stop further data loss or unauthorized access;

investigate how the breach occurred; promptly contact all affected users via email; and contact law enforcement and government agencies when appropriate.

UNITED STATES

- ***Children's Online Privacy Protection Act (COPPA):*** *As a non-profit organization, XtraMath is not subject to COPPA. Nevertheless, we fully comply with the law as if we were subject to it. Children under the age of 13 may not create accounts. We only collect usage and performance data from students as a result of their performing educational activities, and we only use that data for educational purposes. If we gain actual knowledge that a child is using XtraMath without the appropriate consent, we terminate the account.*
- ***Family Education Rights Protection Act (FERPA):*** *Schools in the United States may provide student data to XtraMath while complying with FERPA. When a School provides us with a student's Personal Data (or PII — Personally Identifiable Information) under the FERPA school official exemption, they remain in control of that data. XtraMath will only use and disclose that data as specified in our Terms and as allowed by law.*
- ***General Data Protection Regulation (GDPR):*** *XtraMath affirms and respects all data subject's rights under GDPR. We minimize the data we collect and process, and use data only as described in this policy. For detailed information about what data we process, for what purpose, for how long, and our basis for doing so under the GDPR, see Appendix B, Record of Data Processing. To object to processing, or to request data deletion or access, contact our Data Protection Officer at privacy@xtramath.org.*

Cookies and Local Storage

XtraMath intends to discontinue the use of cookies by August 1, 2018.

XtraMath uses two types of cookies. These cookies can be cleared via browser settings — aboutcookies.org provides cookie management instructions for many specific browsers.

- ***Google Analytics:*** *cookies allow us to see data such as the number of site visitors we get, and which pages they visit the most.*
- ***Vimeo:*** *cookies are stored when users play the videos on our homepage, and primarily keep track of the video player settings.*

The XtraMath website uses "LocalStorage" files to remember a user's sign-in information (if they choose to do so). We also use "SessionStorage" to improve performance during student activities by temporarily storing activity data on the device. Use of LocalStorage and SessionStorage is not required to use XtraMath. Users can remove remembered sign-in information at any time via the appropriate sign-in page. Users can also clear all LocalStorage by using the "Clear now" button on our support page, or via browser settings.

The XtraMath mobile apps use application data for the same purposes as browser LocalStorage and SessionStorage. Users can still remove remembered sign-in information via the app's sign-in pages. Uninstalling the app will remove all locally stored data. Some devices also allow users to clear locally stored app data without uninstalling the app.

Contact Us

For data privacy questions or concerns, to object to processing, or to request access to or deletion of your or your child's Personal Data, email us at privacy@xtramath.org. You may also write to us at: XtraMath, 4700 42nd Ave SW #535, Seattle, WA 98116

Appendix A: List of Third Party Providers

This list will be kept up-to-date to include all third-party providers with which XtraMath shares user data.

Provider Name	Data shared with Provider	Purpose	Relevant Policies
AWS	User account data, including name, email address, and program usage.	Database hosting via remote servers	Privacy Policy
Google	Anonymous ID created by cookie	Public website analytics only, not used in Student application.	Privacy Policy Opt-out Browser Add-on
MaxMind	IP address	Geolocation service	Privacy Policy
Vimeo	Anonymous ID created by cookie, video player settings	Enable playback of embedded videos (remember volume, if video is paused, etc)	Privacy Policy

Appendix B: Record of Data Processing

We have compiled this record in order to provide users with as much transparency as possible into how we use their data. This record also helps us to comply with European law. Unless otherwise noted in the record below, we process user data based on our legitimate interests.

Account Type	Type of Data	Processing Purpose	Deletion
Student	**First name, PIN, parent or teacher email, class**	Account access and identification	Upon account closure[1]. Some information is deleted upon removal from the class or linked account.
	Single-sign-on provider and hashed ID	Account access using optional 3rd party credential	Upon request or account closure[1]
	Grade level	Determine initial activity level. When de-identified and aggregated, used to analyze program usage.	Upon account closure[1]
	Program settings: current program, UI options, preferred language, etc.	Activity customization. When de-identified and aggregated, used to analyze program usage.	Upon account closure[1]
	Activity data	Activity customization and creation of progress reports. When de-identified and aggregated, used to analyze program usage.	Upon account closure[1]. Some data is deleted when user restarts a program. Detailed activity data is deleted after one year.
Parent or Teacher	**Name, "addressed as" name, email address, hashed password**	Account access and identification	Upon account closure[2, 3]
	Email address	Send announcements, alerts, reports, and/or reminders via email	Processing ceases upon request. Data deletion upon account closure[2, 3]
	Email address	Share with linked accounts that have access to same student or class (for increased transparency and security of student data)	Data deletion upon account closure[2, 3]
	Account settings: account type, email	Create progress reports and maintain data preferences	Upon account closure[2, 3]

Account Type	Type of Data	Processing Purpose	Deletion
	preferences, time zone, etc.		
	Electronic identifiers: account change timestamps, version number, etc.	Technical support and account security	Upon account closure[2, 3]
	Single-sign-on provider and hashed ID	Account access using optional 3rd party credential	Upon request or account closure[2, 3]
	IP address	Determine time zone upon sign-up	Not stored
	Hashed IP address	Account security	After 1 year or upon account closure[2, 3]
Teacher	**Hashed IP address**	Expedite classroom setup on multiple devices	After 24 hours
	Class name, class end date, student names	Create progress reports and facilitate program usage	Upon request, account closure[3], or one year after class end date.
All users	**Hashed IP address, change logs**	Network security	After 90 days
	De-identified and aggregated usage data	Product improvement and development, promotional activities, and educational research	Until no longer useful

1. Student accounts: account closure occurs upon request, automatically after two years of account inactivity, or one month after being unlinked from all parent and teacher accounts.
2. Parent accounts: account closure occurs upon request, or automatically after two years of account inactivity.
3. Teacher accounts: account closure occurs upon request.

Current as of July 2022.