

Center for Instruction,
Technology & Innovation

Build Your Future

Services Agreement with the Center for Instruction, Technology &
Innovation (CiTi BOCES)

This Agreement, made this 09/19/2023 (“Effective Date”), by and between the Center for Instruction, Technology and Innovation (“School District”), having an office at 179 County Route 64, Mexico, New York and, Xtramath having an office at 4742 42nd Ave SW #625 Seattle, WA 98116 (collectively the “Parties”).

In consideration of the mutual promises and covenants contained herein, the Parties agree as follows:

1.

Services. Vendor shall perform the services set forth in this Agreement, as described in Addendum C (the “Services”). Vendor shall provide the Services at the School District location or on a remote basis, as agreed to by the Parties. Vendor warrants that the Services provided hereunder will be performed in a good and workmanlike manner.

License. Vendor hereby grants to School District, including to all School District’s authorized users, a non-exclusive, non-sublicensable, non-assignable and royalty-free license to access and use the service (the “Services”) solely for School District’s operations in accordance with the terms of this Agreement.

2. **Term of Services.** This Agreement begins on the Effective Date and will continue for three years unless terminated earlier as set forth herein (the “Term”).

3. **Termination.** This Agreement may be terminated as follows:

- (a) By the School District upon thirty (30) days’ prior written notice to Vendor;
- (b) By the School District immediately in the event of breach by the Vendor;
- (c) By either Party in the event of a Default not cured within the time period set forth in Section 7 herein; and
- (d) By either Party upon written mutual agreement.

4. **Protection of Confidential Data.** Vendor shall provide its Services in a manner which protects Student Data (as defined by 8 NYCRR 121.1(q)) and Teacher or Principal Data (as defined by 8 NYCRR 121.1(r)) (hereinafter “Confidential Data”) in accordance with the requirements articulated under Federal, State and local laws and regulations, including but not limited to the foregoing:

- (a) Vendor will adopt technologies, safeguards and practices that align with the NIST Cybersecurity Framework.

- (b) Vendor will comply with the School District Data Security and Privacy Policy, Education Law § 2-d, and 8 NYCRR §121.
- (c) Vendor will limit internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services.
- (d) Vendor will not use the personally identifiable information for any purpose not explicitly authorized in this Agreement.
- (e) Vendor will not disclose any personally identifiable information to any other party without the prior written consent of the parent or eligible student, unless otherwise authorized pursuant to applicable law.
- (f) Vendor will maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in its custody.
- (g) Vendor will use encryption to protect personally identifiable information in its custody while in motion or at rest.
- (h) Vendor will not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.
- (i) In the event Vendor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the Vendor shall apply to the subcontractor.

6. Data Breach. In the event that Confidential Data is accessed or obtained by an unauthorized individual, Vendor shall provide notification to the School District without unreasonable delay and not more than seven calendar days after the discovery of such breach. Vendor shall follow the following process:

- (a) The security breach notification shall be titled “Notice of Data Breach,” shall be clear, concise, use language that is plain and easy to understand, and to the extent available, shall include: a brief description of the breach or unauthorized release; the dates of the incident and the date of discovery; a description of the types of Confidential affected; an estimate of the number of records affected; a brief description of the vendors investigation or plan to investigate; and contact information for representatives who can assist the School District with additional questions.
- (b) The Vendor shall also prepare a statement for parents and eligible students which provides information under the following categories: “What

Happened,” “What Information Was Involved,” “What We Are Doing,” “What You Can Do,” and “For More Information.”

- (c) Where a breach or unauthorized release of Confidential Data is attributed to Vendor, and/or a subcontractor or affiliate of Vendor, Vendor shall pay for or promptly reimburse the School District for the cost of notification to parents and eligible students of the breach.
- (d) Vendor shall cooperate with the School District and law enforcement to protect the integrity of investigations into the breach or unauthorized release of Confidential Data.
- (e) Vendor further acknowledges and agrees to have a written incident response plan that is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Protected Data or any portion thereof. Upon request, Vendor shall provide a copy of said written incident response plan to the School District.

7. Indemnification. Vendor shall at all times (both during and after the Term of this Agreement), indemnify, defend and hold harmless the School District, its agents, employees and students (collectively for purposes of this Section “the School District”), from and against any and all settlements, losses, damages, costs, counsel fees and all other expenses relating to or arising from (a) Vendor’s failure to comply with the terms of this Agreement; and/or (b) the negligent operations, acts or omissions of the Vendor.

8. Assignment. This Agreement is binding upon the Parties and their respective successors and assigns, but Vendor’s obligations under this Agreement are not assignable without the prior written consent of the School District. Any assignment without the School District’s consent shall be null and void.

9. Default. The School District shall be in Default under this Agreement if the School District fails to pay any fees or charges or any other payments required under this Agreement when due and payable, and such failure continues for a period of fifteen (15) days after receipt written notification of such failure. The Vendor shall be in default of this Agreement if it becomes insolvent, dissolves, or assigns its assets for the benefit of its creditors, or files or has filed against it any bankruptcy or reorganization proceeding.

10. Intellectual Property. Intellectual property rights arising from the Services (but not the data, materials or content provided by Client) shall remain the property of Vendor, and nothing contained in any work product shall be construed to transfer, convey, restrict, impair or deprive Vendor of any of its ownership or proprietary interest or rights in technology, information or products that existed prior to the provision of deliverables under this Agreement or that may be independently developed by Vendor outside the scope of the services provided

under this Agreement and without use of any confidential or otherwise restricted material or information thereunder.

11. Governing Law. This Agreement and any Services procured hereunder shall be governed by the laws of the State of New York both as to interpretation and performance, without regard to its choice of law requirements. Each party consents and submits, for any dispute arising out of or relating to this Agreement or the transactions contemplated hereby, to the sole and exclusive jurisdiction of the state and federal courts located in the county in which the School District is located.

12. Compliance with Laws. Vendor, its employees and representatives shall at all times comply with all applicable Federal, State and local laws, rules and regulations.

13. Independent Relationship. It is expressly intended by the Parties hereto, and Vendor hereby specifically warrants, represents and agrees, that Vendor and the School District are independent entities. The Parties intend that this Agreement is strictly between two independent entities and does not create an employer/employee relationship for any purpose. Vendor shall perform the duties contemplated by this Agreement as an independent entity, to whom no benefits shall accrue except for those benefits expressly set forth in this Agreement.

14. Public Inspection of Agreement. Vendor acknowledges and agrees that this Agreement and all documents Vendor provides to School District as required herein, are public records and may at all times be subject to public inspection.

15. Waiver. No delay or omission of the School District to exercise any right hereunder shall be construed as a waiver of any such right and the School District reserves the right to exercise any such right from time to time, as often as may be deemed expedient.

16. Addendums. The following Addendums are attached hereto and incorporated herein:

- Addendum A: Parents' Bill of Rights for Data Privacy and Security
- Addendum B: Parents' Bill of Rights – Supplemental Information Addendum
- Addendum C: Product Specifications and Product Table
- Addendum D: Vendor's Data Security and Privacy Plan
- Addendum E: Schedule of Data
- Addendum F: Joinder Agreement

17. Severability. Should any part of this Agreement for any reason be declared by any court of competent jurisdiction to be invalid, such decision shall not affect the validity of any remaining portion, which remaining portion shall continue in full force and effect as if this Agreement had been executed with the invalid portion hereof eliminated, it being the intention of the Parties that they would have executed the remaining portion of this Agreement without including any such part, parts or portions which may for any reason be hereafter declared invalid.

18. Entire Agreement. This Agreement and its attachment constitute the entire Agreement between the Parties with respect to the subject matter hereof and shall supersede all

previous negotiations, commitments and writings. It shall not be released, discharged, changed or modified except by an instrument in writing signed by a duly authorized representative of each of the Parties.

IN WITNESS WHEREOF, the parties have executed this Agreement intending to be legally bound.

Center for Instruction, Technology and Innovation (CiTi BOCES)

Michael Sheperd
Michael Sheperd (Sep 20, 2023 11:05 EDT)

Signature

Michael Sheperd

Printed Name

Assistant Superintendent

Title

XtraMath

Roy King

Signature

Roy King

Printed Name

Executive Director

Title

Addendum A

CiTi BOCES PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

Parents (includes legal guardians or persons in parental relationships) and Eligible Students (student 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any commercial purpose. PII, as defined by Education Law § 2-d and FERPA, includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.

2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency. This right may not apply to parents of an Eligible Student.

3. State and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, the Family Educational Rights and Privacy Act ("FERPA") at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student's identifiable information.

4. Safeguards associated with industry standards and best practices including but not limited to encryption, firewalls and password protection must be in place when student PII is stored or transferred.

5. A complete list of all student data elements collected by NYSED is available at

<http://www.nysed.gov/data-privacy-security/student-data-inventory> and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.

6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. Complaints may be submitted to NYSED at <http://www.nysed.gov/data-privacy-security/report-improper-disclosure>, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to privacy@nysed.gov; or by telephone at 518-474- 0937. Complaints regarding student data breaches can also be directed to: Kristen Foland, Director of Instructional Support Services, Center for Instruction, Technology & Innovation, 179 County Route 64, Mexico NY, 13114. Phone: 315-963-4425 email: kfoland@citiboces.org.

7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII

occurs.

8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.

9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

Addendum B

PARENTS' BILL OF RIGHTS – SUPPLEMENTAL INFORMATION ADDENDUM

1. As used in this Addendum B, the following terms will have the following meanings:
 - a. “Student” shall have the meaning defined in Subsection 1(f) of Section 2-d.
 - b. “Eligible Student” shall have the meaning defined in Subsection 1(g) of Section 2-d.
 - c. “Personally Identifiable Information” as applied to Student Data shall have the meaning defined in Subsection 1(d) of Section 2-d.
 - d. “Student Data” means Personally Identifiable Information from student records that Vendor receives from CiTi BOCES.

Other capitalized terms used in this Addendum B will have the applicable meaning set forth elsewhere in this Agreement or in Section 2-d.

2. Vendor agrees that the confidentiality of Student Data shall be maintained in accordance with state and federal laws that protect the confidentiality of Student Data.
3. Vendor agrees that any of its officers or employees, and any officers or employees of any assignee of Vendor, who have access to Student Data will be provided training on the federal and state law governing confidentiality of such Student Data prior to receiving access to that data.
4. The exclusive purpose for which Vendor is being provided access to Student Data is to permit Vendor to provide Services as set forth in the Agreement. Student Data received by Vendor, or by any assignee of Vendor or third party contracting with Vendor, shall not be sold or used for marketing purposes.
5. If Vendor comes into possession of Student Data, Vendor will only share such Student Data with additional third parties if those third parties are contractually bound to adhere to data protection and security requirements, including but not limited to those outlined in applicable state and federal laws and regulations (e.g., Family Educational Rights and Privacy Act (“FERPA”); Education Law §2-d; 8 NYCRR Part 121).
6. 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 CiTi BOCES in [insert data format] format and/or destroyed by the Contractor as directed by CiTi BOCES.

7. If a parent, Student, or Eligible Student wishes to challenge the accuracy of any “education record”, as that term is defined in the FERPA, by following the School District’s procedure for requesting the amendment of education records under the FERPA. Teachers and principals may be able to challenge the accuracy of APPR data stored by CiTi BOCES in Contractor’s product and/or service by following the appeal procedure in the School District’s APPR Plan. Unless otherwise required above or by other applicable law, challenges to the accuracy of the Confidential Data shall not be permitted.

8. Student Data transferred to Vendor by CiTi BOCES will be stored in electronic memory (on servers or other computers) operated and maintained by or on behalf of Vendor in the United States. The measures that Vendor will take to protect the privacy and security of Student Data while it is stored in that manner include, but are not necessarily limited to: encryption to the extent required by Section 2-d; restricted physical access to the servers/computers; software-based solutions intended to prohibit unauthorized entry such as regularly updated virus scans, firewalls, and use of passwords; and administrative controls such as selective user access rights. The measures that Vendor takes to protect Confidential Data will align with the NIST Cybersecurity Framework.

9. 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.

Addendum C

PRODUCT SPECIFICATIONS AND PRICING TABLE

Description of Services XtraMath® Premium Program, is an online math fact fluency paid subscription program that helps students develop quick recall and automaticity of their basic math facts.

Product Specifications XtraMath is a Software as as Service, online math fact fluency program that users log into and runs on laptops, tablets, ipads

Product Table

Product Description
XtraMath Free
XtraMath Family
XtraMath Teacher
XtraMath School

Addendum D

VENDOR'S DATA SECURITY AND PRIVACY PLAN

<https://home.xtramath.org/privacy>

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. In Appendix B, Record of Data Processing, we summarize the data we collect on students, teachers, and parents. It includes an up-to-date list of what user data we collect, and how we use that data,

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.

STUDENT DATA

A student's Personal Data is collected and used by our application logic to provide each student with the 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

XtraMath has never and will never release, trade, or sell anyone's Personal Data to any third-party advertising. 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 required by law or a court order.

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.

In the event of a joint venture, sale or merger with another party is approved by our Board of Directors. In that case, the third party would still be required to uphold our Terms, including our Privacy Policy for all existing accounts. We would provide advance notice before any accounts were shared with the third party.

USE OF DE-IDENTIFIED DATA

We may use de-identified usage data internally to improve our educational services and develop new products. We will never attempt to re-identify data that has been de-identified. We may use aggregate de-identified data, such as the number of users of our service, for promotional purposes.

We may use de-identified data along with professional 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.

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.

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 may provide certification of data deletion upon request.

DATA BREACH RESPONSE

Compliance with Data Privacy Laws

We use industry-standard practices to safeguard all data including 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.

Local Storage

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 student's Personal Data, email us at privacy@xtramath.org. You may also write to us at:

XtraMath, 4742 42nd Ave SW #625 Seattle, WA 98116

Addendum E

SCHEDULE OF DATA

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses, Use of cookies etc.	✓
	Other application technology meta data Specify:	
Application Use Statistics	Meta data on user interaction with application	✓
Assessment	Standardized test scores	
	Observation data	
	Other assessment data (specify): <i>Student Personality Assessments</i>	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications that are captured (emails, blog entries)	
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, preferred or primary language spoken by student)	
	Other demographic information Specify:	
Enrollment	Student school enrollment	✓
	Student grade level	✓
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information (specify):	
Parent/Guardian Contact Information	Address	
	Email	✓
	Phone	
Parent/Guardian ID	Parent ID number (created to link parents to students)	✓
Parent/Guardian Name	First and/or Last	✓

Category of Data	Elements	Check if used by your system
Schedule	Student scheduled courses	
	Teacher names	
Special Indicator	English language learner information	
	Low income status	
	Medical alerts	
	Student disability information Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information(specify): <i>First Generation College Student</i>	
Student Contact Information	Address	
	Email	
	Phone	
Student Identifiers	Local (School district) ID number	
	State ID number	
	Vendor/App assigned student ID No.	✓
	Student app username	✓
	Student app passwords	✓
Student Name	First and/or Last	✓
Student In-App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	✓
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	
Student work	Student generated content; writing, pictures etc.	
	Other student work data Please specify:	
Transcript	Student course grades	
	Student course data	
	Student course grades/performance scores	

Category of Data	Elements	Check if used by your system
	<p align="center">Other transcript data Please specify:</p>	
Transportation	<p align="center">Student bus assignment</p>	
	<p align="center">Student pick up and/or drop off location</p>	
	<p align="center">Student bus card ID number</p>	
	<p align="center">Other transportation data Please specify:</p>	
Other	<p align="center">Please list each additional data element used, stored or collected by your application</p>	

Addendum F
JOINDER AGREEMENT

This Joinder Agreement (“Joinder”) is effective as of the date of signature below and is entered into by the undersigned Participating School pursuant to that certain Agreement, dated March 1, 2022 by and between XtraMath and Center for Instruction, Technology and Innovation (the “Agreement”). Capitalized terms used but not defined in this Joinder shall have the respective meanings ascribed to such terms in the Agreement. By the execution of this Joinder, the Participating School (i) agrees to be bound by, and subject to, the terms and conditions of the Agreement as a “Participating School” and a “Party” thereunder, (ii) adopts the Agreement with the same force and effect as if the Participating School was originally a party thereto, and (iii) agrees that any Confidential Data provided by the Participating School to Vendor shall be governed by the Agreement.

The Agreement shall extend only to the data privacy and security matters that are the subject matter thereof and the Terms shall continue to govern with respect to all other matters. In the event of a conflict or an inconsistency between the terms and conditions of the Terms and the terms and conditions of the Agreement, the Agreement shall govern and control.

In order for this Joinder to be effective, the Participating School must send a signed copy of this Joinder to Center for Instruction, Technology and Innovation via email to Acanale@citiboces.org or by mail to 179 County Route 64 Mexico NY, 13114 and to XtraMath via email at privacy@xtramath.org or by mail to 4742 42nd Ave SW #625 Seattle, WA 98116.

Name of Participating School: CITI BOCES on behalf of Sandy Creek CSD

By: _____

Name: _____

Title: _____

Date: _____

Address: _____






XtraMath ED Law MSA Vendor Signed

Final Audit Report

2023-09-20

Created:	2023-09-20
By:	Anthony Canale (acanale@citiboces.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAA-OTg66IA-WBtZR1IG6pqm-jivFCyz8U1

"XtraMath ED Law MSA Vendor Signed" History

-  Document created by Anthony Canale (acanale@citiboces.org)
2023-09-20 - 2:12:34 PM GMT- IP address: 104.229.82.246
-  Document emailed to Michael Sheperd (msheperd@citiboces.org) for signature
2023-09-20 - 2:13:37 PM GMT
-  Email viewed by Michael Sheperd (msheperd@citiboces.org)
2023-09-20 - 3:04:12 PM GMT- IP address: 104.47.58.126
-  Document e-signed by Michael Sheperd (msheperd@citiboces.org)
Signature Date: 2023-09-20 - 3:05:07 PM GMT - Time Source: server- IP address: 170.158.39.8
-  Agreement completed.
2023-09-20 - 3:05:07 PM GMT