

EXHIBIT D

DATA SHARING AND CONFIDENTIALITY AGREEMENT

INCLUDING
PARENTS BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY
AND
SUPPLEMENTAL INFORMATION ABOUT THE MLSA

1. **Purpose**

- (a) This Exhibit supplements the Master License and Service Agreement (“MLSA”) to which it is attached, to ensure that the MLSA conforms to the requirements of New York State Education Law Section 2-d and any implementing Regulations of the Commissioner of Education (collectively referred to as “Section 2-d”). This Exhibit consists of the terms of this Data Sharing and Confidentiality Agreement, a copy of Erie 1 BOCES’ Parents Bill of Rights for Data Security and Privacy signed by the Vendor, and the Supplemental Information about the MLSA that is required to be posted on Erie 1 BOCES’ website.
- (b) To the extent that any terms contained within the MLSA, or any terms contained within any other Exhibits attached to and made a part of the MLSA, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect. In the event that Vendor has online or written Terms of Service (“TOS”) that would otherwise be applicable to its customers or users of its Product that is the subject of the MLSA, to the extent that any term of the TOS conflicts with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect.

2. **Definitions**

Any capitalized term used within this Exhibit that is also found in the MLSA will have the same definition as contained within the MLSA.

In addition, as used in this Exhibit:

- (a) “Student Data” means personally identifiable information, as defined in Section 2-d, from student records that Vendor receives from a Participating Educational Agency pursuant to the MLSA.
- (b) “Teacher or Principal Data” means personally identifiable information relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of New York Education Law Sections 3012-c or 3012-d, that Vendor receives from a Participating Educational Agency pursuant to the MLSA.
- (c) “Protected Data” means Student Data and/or Teacher or Principal Data to the extent applicable to Vendor’s Product.

- (d) "Participating Educational Agency" means a school district within New York State that purchases certain shared instructional technology services and software through a Cooperative Educational Services Agreement with a BOCES, and as a result is licensed to use Vendor's Product pursuant to the terms of the MLSA. For purposes of this Exhibit, the term also includes Erie 1 BOCES or another BOCES that is licensed to use Vendor's Product pursuant to the MLSA to support its own educational programs or operations.

3. **Confidentiality of Protected Data**

- (a) Vendor acknowledges that the Protected Data it receives pursuant to the MLSA may originate from several Participating Educational Agencies located across New York State, and that this Protected Data belongs to and is owned by the Participating Educational Agency from which it originates.
- (b) Vendor will maintain the confidentiality of the Protected Data it receives in accordance with federal and state law (including but not limited to Section 2-d) and Erie 1 BOCES's policy on data security and privacy. Vendor acknowledges that Erie 1 BOCES is obligated under Section 2-d to adopt a policy on data security and privacy.. Erie 1 BOCES will provide Vendor with a copy of its policy. Vendor and Erie 1 BOCES agree to engage in good faith negotiations to modify this Data Sharing Agreement to the extent necessary to ensure Vendor's continued compliance with Section 2-d.

4. **Data Security and Privacy Plan**

Vendor agrees that it will protect the confidentiality, privacy and security of the Protected Data received from Participating Educational Agencies in accordance with Erie 1 BOCES' Parents Bill of Rights for Data Privacy and Security, a copy of which has been signed by the Vendor and is set forth below.

Additional elements of Vendor's Data Security and Privacy Plan are as follows:

- (a) In order to implement all state, federal, and local data security and privacy requirements, including those contained within this Data Sharing and Confidentiality Agreement, consistent with Erie 1 BOCES' data security and privacy policy, Vendor will: Review its data security and privacy policy and practices to ensure that they are in conformance with all applicable federal, state, and local laws and the terms of this Data Sharing and Confidentiality Agreement. In the event Vendor's policy and practices are not in conformance, the Vendor will implement commercially reasonable efforts to ensure such compliance.

In order to protect the security, confidentiality and integrity of the Protected Data that it receives under the MLSA, Vendor will have the following reasonable administrative, technical, operational and physical safeguards and practices in place throughout the term of the MLSA:

[See Data Privacy and Security Plan attached](#)

- (b) Vendor will comply with all obligations set forth in Erie 1 BOCES' "Supplemental Information about the MLSA" below.
- (c) For any of its officers or employees (or officers or employees of any of its subcontractors or assignees) who have access to Protected Data, Vendor has provided or will provide training on the federal and state laws governing confidentiality of such data prior to their receiving access, as follows: Annually, Vendor will require that all of its employees (or officers or employees of any of its subcontractors or assignees) undergo data security and privacy training to ensure that these individuals are aware of and familiar with all applicable data security and privacy laws.
- (d) Vendor _____ will will not utilize sub-contractors for the purpose of fulfilling one or more of its obligations under the MLSA. In the event that Vendor engages any subcontractors, assignees, or other authorized agents to perform its obligations under the MLSA, it will require such subcontractors, assignees, or other authorized agents to execute written agreements as more fully described in Erie 1 BOCES' "Supplemental Information about the MLSA," below.
- (e) Vendor will manage data security and privacy incidents that implicate Protected Data, including identifying breaches and unauthorized disclosures, and Vendor will provide prompt notification of any breaches or unauthorized disclosures of Protected Data in accordance with Section 6 of this Data Sharing and Confidentiality Agreement.
- (f) Vendor will implement procedures for the return, transition, deletion and/or destruction of Protected Data at such time that the MLSA is terminated or expires, as more fully described in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

5. **Additional Statutory and Regulatory Obligations**

Vendor acknowledges that it has the following additional obligations with respect to any Protected Data received from Participating Educational Agencies, and that any failure to fulfill one or more of these statutory or regulatory obligations shall be a breach of the MLSA and the terms of this Data Sharing and Confidentiality Agreement:

- (a) Limit internal access to education records to those individuals that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA).
- (b) Limit internal access to Protected Data to only those employees or subcontractors that need access in order to assist Vendor in fulfilling one or more of its obligations under the MLSA.
- (c) Not use education records for any purposes other than those explicitly authorized in this Data Sharing and Confidentiality Agreement.
- (d) Not disclose any personally identifiable information to any other party, except for authorized representatives of Vendor using the information to carry out Vendor's obligations under the MLSA, unless:

- (i) the parent or eligible student has provided prior written consent; or
 - (ii) the disclosure is required by statute or court order and notice of the disclosure is provided to Participating Educational Agency no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order.
- (e) Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of personally identifiable student information in its custody;
- (f) Use encryption technology that complies with Section 2-d, as more fully set forth in Erie 1 BOCES' "Supplemental Information about the MLSA," below.
- (g) Provide notification to Erie 1 BOCES (and Participating Educational Agencies, to the extent required by, and in accordance with, Section 6 of this Data Sharing and Confidentiality Agreement) of any breach of security resulting in an unauthorized release of Protected Data by Vendor or its assignees or subcontractors in violation of state or federal law or other obligations relating to data privacy and security contained herein.
- (h) Promptly reimburse Erie 1 BOCES, another BOCES, or a Participating School District for the full cost of notification, in the event they are required under Section 2-d to notify affected parents, students, teachers or principals of a breach or unauthorized release of Protected Data attributed to Vendor or its subcontractors or assignees.

6. **Notification of Breach and Unauthorized Release**

- (a) Vendor shall promptly notify Erie 1 BOCES of any breach or unauthorized release of Protected Data in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after Vendor has discovered or been informed of the breach or unauthorized release.
- (b) Vendor will provide such notification to Erie 1 BOCES by contacting Michelle Okal-Frink directly by email at mokal@e1b.org, or by calling (716) 821-7200 (office) or (716) 374-5460 (cell).
- (c) Vendor will cooperate with Erie 1 BOCES and provide as much information as possible directly to Michelle Okal-Frink or her designee about the incident, including but not limited to: a description of the incident, the date of the incident, the date Vendor discovered or was informed of the incident, a description of the types of personally identifiable information involved, an estimate of the number of records affected, the Participating Educational Agencies affected, what the Vendor has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data, and contact information for Vendor representatives who can assist affected individuals that may have additional questions.
- (d) Vendor acknowledges that upon initial notification from Vendor, Erie 1 BOCES, as the educational agency with which Vendor contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department

("CPO"). Vendor shall not provide this notification to the CPO directly. In the event the CPO contacts Vendor directly or requests more information from Vendor regarding the incident after having been initially informed of the incident by Erie 1 BOCES, Vendor will promptly inform Michelle Okal-Frink or her designees.

- (e) Vendor will consult directly with Michelle Okal-Frink or her designees prior to providing any further notice of the incident (written or otherwise) directly to any other BOCES or Regional Information Center, or any affected Participating Educational Agency.

EXHIBIT D (CONTINUED)**PARENTS BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY**

Erie 1 BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, the BOCES wishes to inform the community of the following:

- (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.
- (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 for public review at <http://www.nysed.gov/data-privacy-security/student-data-inventory>, or 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, 89 Washington Avenue, Albany, New York 12234. Complaints may also be submitted using the form available at the following website <http://www.nysed.gov/data-privacy-security/report-improper-disclosure>.

BY THE VENDOR:

DocuSigned by:

C7/B734D018464C8...
Signature**Paul Marvin**
Printed Name**Interim CFO**
Title**Date** 7/19/2023

EXHIBIT D (CONTINUED)

SUPPLEMENTAL INFORMATION

ABOUT THE MASTER LICENSE AND SERVICE AGREEMENT
BETWEEN
ERIE 1 BOCES AND DREAMBOX LEARNING, INC

Erie 1 BOCES has entered into a Master License and Service Agreement (“MLSA”) with DreamBox Learning, Inc which governs the availability to Participating Educational Agencies of the following Product(s):

DreamBox Math
Reading Plus
Reading Park

Pursuant to the MLSA, Participating Educational Agencies may provide to Vendor, and Vendor will receive, personally identifiable information about students, or teachers and principals, that is protected by Section 2-d of the New York State Education Law (“Protected Data”).

Exclusive Purpose for which Protected Data will be Used: The exclusive purpose for which Vendor is being provided access to Protected Data is to provide Participating Educational Agencies with the functionality of the Product(s) listed above. Vendor agrees that it will not use the Protected Data for any other purposes not explicitly authorized in the MLSA. Protected Data received by Vendor, or any of Vendor’s subcontractors, assignees, or other authorized agents, will not be sold, or released or used for any commercial or marketing purposes.

Oversight of Subcontractors: In the event that Vendor engages subcontractors, assignees, or other authorized agents to perform one or more of its obligations under the MLSA (including any hosting service provider), it will require those to whom it discloses Protected Data to execute legally binding agreements acknowledging the obligation under Section 2-d of the New York State Education Law to comply with the same data security and privacy standards required of Vendor under the MLSA and applicable state and federal law. Vendor will ensure that such subcontractors, assignees, or other authorized agents abide by the provisions of these agreements by: DreamBox does not utilize subcontractors.

Duration of MLSA and Protected Data Upon Expiration:

- The MLSA commences on July 1, 2023 and expires on June 30, 2026.
- Upon expiration of the MLSA without renewal, or upon termination of the MLSA prior to expiration, Vendor will securely delete or otherwise destroy any and all Protected Data remaining in the possession of Vendor or its assignees or subcontractors or other authorized persons or entities to whom it has disclosed Protected Data. If requested by Erie 1 BOCES and/or any Participating Educational Agency, Vendor will assist a Participating Educational Agency in exporting all Protected Data previously received back

to the Participating Educational Agency for its own use, prior to deletion, in such formats as may be requested by the Participating Educational Agency.

- In the event the Master Agreement is assigned to a successor Vendor (to the extent authorized by the Master Agreement), the Vendor will cooperate with Erie 1 BOCES as necessary to transition Protected Data to the successor Vendor prior to deletion.
- Neither Vendor nor any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data will retain any Protected Data, copies, summaries or extracts of the Protected Data, or any de-identified Protected Data, on any storage medium whatsoever. Upon request, Vendor and/or its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data, as applicable, will provide Erie 1 BOCES with a certification from an appropriate officer that these requirements have been satisfied in full. Provider may use de-identified, aggregated Play Data for product development and research purposes.

Challenging Accuracy of Protected Data: Parents or eligible students can challenge the accuracy of any Protected Data provided by a Participating Educational Agency to Vendor, by contacting the student's district of residence regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or principals may be able to challenge the accuracy of APPR data provided to Vendor by following the appeal process in their employing school district's applicable APPR Plan.

Data Storage and Security Protections: Any Protected Data Vendor receives will be stored on systems maintained by Vendor, or by a subcontractor under the direct control of Vendor, in a secure data center facility located within the United States. The measures that Vendor will take to protect Protected Data include adoption of technologies, safeguards and practices that align with the NIST Cybersecurity Framework and industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.

Encryption of Protected Data: Vendor (or, if applicable, its subcontractors) will protect Protected Data in its custody from unauthorized disclosure while in motion or at rest, using a technology or methodology specified by the secretary of the U.S. Department of HHS in guidance issued under Section 13402(H)(2) of P.L. 111-5.

From www.dreambox.com/privacy-policy



Who We Are and What We Do
July 8, 2022

DreamBox Learning® (DreamBox), the leading K-12 education technology provider in the world learns. As the only dual-discipline solution rated “Strong” by Johns Hopkins University, DreamBox uniquely provides schools high-quality, adaptive mathematics and reading, DreamBox independently proven to accelerate student growth. We built DreamBox because every child deserves to learn, no matter where they start, where they live, or who they are. We are dedicated to helping students realize their potential, working together with parents, guardians, teachers, principals, and district administrators. Critical to our vision is safeguarding the privacy of every person who uses DreamBox. You can learn more about our company values [here](#).

Privacy Statement

In this policy, we’ve attempted to provide as much useful information as possible, from many different angles, to help you find whatever answers you might need about our approach to privacy. But, at the core, our approach to privacy is this:

DreamBox understands that your data is important, personal, and that it is yours. You shared your data with us so that we can provide you with the DreamBox service, but we don’t own the data: you do. We will not use the data you share to use our services for third-party marketing or other unrelated purposes. We won’t sell it to or share it with any company not directly involved in providing the DreamBox service or services you are using. We will always protect your data, using world-class security measures and practices implemented by vetted, fully-trained personnel. We will be transparent about exactly what data we have from you or about you, how we got that data, and how we use it. If you ask us to delete your data, we will remove you from the DreamBox services, destroy your personal data, and alert you when your removal is complete. We will not collect additional personal information directly from children, or market products to children using the data you provide. See also our statement about Student Privacy, directly below this note.

Student Privacy

DreamBox Learning is deeply committed to setting a high bar for protecting students’ privacy and sensitive student information across all our learning products. We believe that students, educators, and learning guardians benefit when there is trust in learning. We believe that well-conceived privacy policies and rigorous enforcement of those policies are a core requirement for online learning. As evidence of our commitment to these principles, we’ve signed on to the nationwide Student Privacy Pledge 2020.

For students who use our system, we receive information from a school or school district, or a parent or learning guardian. When students use our system, they generate usage and performance data that capture how students interact with lessons. We use that statistical data to measure performance, adapt programs to each student’s learning needs, and provide progress reports to educators and learning guardians. We do not collect personal information from students at any time.

We do not market products to students, either within our services or elsewhere. When schools and learning guardians provide student data to use our services, we do not use that data for direct marketing, third-party marketing, or any other unrelated purposes. We will not sell it to or share it with any company not directly involved in providing DreamBox services.

Why we have your information

DreamBox has your information for one of these reasons:

You or your parent or guardian signed up for the DreamBox service

An authorized educational institution (a school or school district) shared information about you with DreamBox.

For the cases above, we only use your data for the express purpose of providing you the educational service that you, your guardian or your school signed up for. This may include notices about updates and changes to the functionality of the service, or ways in which you can more fully take advantage of the service’s features.

If you provide information when inquiring about our products on one of our marketing sites: www.dreambox.com , www.readingplus.com or www.squigglepark.com, we will use this data to contact you with information about becoming a DreamBox customer.

Definitions of some terms used in this policy

Individual Customer or customers that are individuals: individuals or families who directly purchased the DreamBox service for personal or family use.

Individual Parent: a parent or guardian of a student who directly signed their student up to use the DreamBox service.

(In other words, their student was not signed up by a school or district.)

Parent: a parent or guardian of a student using the DreamBox service, regardless of how the student was signed up for DreamBox services.

School Customer: an educational institution that has purchased the DreamBox service and provisions accounts for individual student users.

School Parent: a parent or guardian of a student using the DreamBox service, who has been signed up by a school or district.

Student User: any individual using the DreamBox service, whether signed up by a parent or a school. Students may be any age, but DreamBox treats all students as though they are covered by legal protections for children aged 13 or younger.

The Information We Collect from Customers

Parent's First and Last Name: You will need to provide a first and last name to access the parent dashboard to track your student's progress. For Individual Customers, first and last name may also be required by our payment processor for initial processing of credit card payments.

Email Address: For customers who are parents and school administration officials, your email address will serve as your login username (For customers that are individuals or students, your name or other identifier set up at registration, or a picture identifier chosen after registration, will serve as your login username.) Your email address may be used to send a confirmation email at registration, as well as information and updates to the DreamBox Service. In some cases, we will also email your student's personal reports to you, with further information about the progress your student is making. We may use the email address as an additional means of communicating with you about the Programs and DreamBox Learning, including notifying you of updates to websites or policies.

Phone Number: Your phone number will serve as an alternate way of contacting you for the same purposes as the email address. Providing a phone number is optional for Parents using the parent dashboard, though it may be required by our payment processor for initial processing of credit card payments. We do not collect phone numbers for students, and we will never call a student directly.

Student's First and Last Name: Your student's name will be used to customize your student's participation in the Programs, and to personalize reports and updates about your student's progress. Also, for Individual Customers, we may mail related material to you or your student using your name or his/her name, care of you, at the mailing address you provide.

Student's Date of Birth: If provided, we will use a student's age to group Performance Data (See "The Information We Collect from Children," below) of children of similar age, to assess relative performance and improve the program. Such information will be aggregated with other customers in an anonymous manner and will not include any information that could be used to identify a specific student.

Student's School Grade Level: We will use a student's grade level to group Performance Data of children of similar grade, to assess relative performance and improve the program. Such information will be aggregated with other customers in an anonymous manner and will not include any information that could be used to identify a specific student.

Demographic data: We allow our school customers to supply demographic information to aid them in monitoring and advancing equity efforts, and to verify compliance with state, jurisdiction, and school district requirements. This type of information is not collected from consumer customers, nor is it required from any customer.

This demographic information is only used by school employees and DreamBox staff to support those equity efforts. It is never used by DreamBox for any other purpose. The types of demographic data that we currently support as optional inputs from our school customers include:

- race
- gender
- SPED status
- ELL status
- assisted lunch status

Parent's Mailing Address: Your mailing address may be used to allow DreamBox Learning to mail you various Program materials and ancillary program products. At a minimum, you must provide a postal code to use the Programs. Providing a street address is optional, though a full address including postal code may be required by our payment

processor for initial processing of credit card payments. We will never collect this information from a student. We will never knowingly contact a student directly.

Credit Card Information: For our customers that are individuals, we may ask for your credit card information to bill you for each student that you register for the Programs. Credit card processing may require:

Credit Card Number
Credit Card Expiration Date
First and Last Name
Billing Address including Postal Code
Phone Number

This information is never handled directly by DreamBox or stored on any of our systems. All credit card information is processed and stored by our processing partner, Stripe.com. Their privacy policy can be found here: <https://stripe.com/privacy>.

Secondary Uses: DreamBox Learning WILL NOT sell, trade, or assign any personal information we collect to third parties outside of DreamBox Learning nor will we ever directly target any type of communication to a student unless specifically requested by you to do so. DreamBox will not use your personal information, or your student's personal information, to target advertising at you, or to market products to you.

The Information We Collect from Students

Participation History: Participation History (how often and how much a customer uses the service and its features) will be collected for customer support, product development, marketing, and other operational and business purposes, including improvements to the Programs; however, such information will not be disclosed to third parties or used for advertising to student users. To be clear: we will not use your student's participation history to market or sell other products to parents.

Performance Data: DreamBox Learning collects information directly from your student, over the Internet, in the form of the interactions that your student makes when participating in the Programs. We refer to the resulting information as "Performance Data," and it includes but is not limited to data on when your student starts and stops a lesson, the responses your student makes to questions asked, the timing of your student's responses, your student's choice of character and customizations, and the choice of lessons to play.

We will use Performance Data to:

Measure your student's performance in each lesson of the DreamBox Learning Programs and to adapt the Programs to his or her learning needs
Analyze your student's Performance Data, and provide you with periodic progress reports about your student's performance in the Programs
Improve the Programs.

DreamBox Learning does not collect personal information directly from students. DreamBox Learning will seek clear, informed authorization of a parent or guardian first if we ever need to collect information (other than Performance Data) directly from a student.

We may aggregate your student's Performance Data with the Performance Data of other students participating in the Programs for marketing and other business-related purposes. Aggregate information will be ANONYMOUS and will not identify your student or be combined with other information that would allow individual students to be identified. It cannot be "de-anonymized" or otherwise connected back to individual students.

Our Rules about Collecting Information Directly from Children

DreamBox Learning does not collect personal information directly from children under 13, or from any student. Personal information about children that we receive, process or store comes from one of two sources: parents who share information about their children, or schools and districts who share information about the students in their charge. If we ever need to collect personal information from children, we will do so only after receiving explicit permission from their parents or guardians.

How does DreamBox use Aggregated and Anonymous Information

Anonymized and aggregated information may be used for demographic profiling and advertising. In such cases, the information will always be aggregated and anonymous. Information used this way will never have a connection to any

individual, or any personal identifier attached to it. It will not be possible to reverse the process and connect this aggregated information to individuals.

How We Protect Information

DreamBox takes great care to ensure we don't misuse your data, or abuse the trust you placed in us when you shared that data. A significant part of our commitment to your privacy is the way we keep your data out of the wrong hands, either through accidental disclosure or the efforts of hostile actors. DreamBox Learning has multiple security measures in place to protect the information under our control against loss, misuse, or alteration.

Laws and guidelines that apply

DreamBox Learning complies with and enforces U.S. data protection laws across all aspects of our system. By signing up for or using the DreamBox Learning system, you agree:

That your personal data can be used for the purposes identified in the Privacy Policy.

That your data will be handled in accordance with U.S. privacy law. You waive any right or expectation enumerated under the data protection laws of other jurisdictions, and consent to the application of U.S. data protection law.

Some regions, such as the EU, do not permit you (the Customer) to grant this consent. DreamBox Learning is not currently available to customers in those jurisdictions.

DreamBox follows ISO 27001 and 27002 guidance for security structures, policies, and procedures.

Our ISO compliance is reviewed annually by an external audit and certification process, and continually through internal processes and checks.

We also refer to guidance from other sources, where those do not directly conflict with ISO 27001 standards. We measure our processes against

NIST SP 800-53 Rev. 4 and to some degree the draft of Rev. 5.

The OWASP Top 10 and other output from OWASP.

HITRUST CSF v9.2.

How we protect information we store

If you use or access the DreamBox system, please note:

Your data will be stored in the United States.

Your data is always stored in an encrypted format. Encryption is done using a 256-bit symmetric key created by DreamBox and accessible only by DreamBox core operations staff.

Your data is always stored in a protected network zone, isolated from employee systems, unprotected networks, and the public Internet.

Backups and archives that include your data are also encrypted with a 256-bit symmetric key, and stored in protected network zones.

How We Protect Information During Transmission

Information being sent to or retrieved from our service

Registration details ("Roster Information") sent through Clever.com are encrypted in transit using certificates, key exchange methods and cipher suites rated "A" or "A+." Currently, that means an RSA 2048 bit key, using SHA256 with RSA, but Clever is continually reviewing best practices and updating their configuration to stay current. Clever's own privacy policy can be found here: <https://clever.com/about/privacy-policy>.

Registration details ("Roster Information") uploaded to, and reports downloaded from our ExaVault SFTP partner are encrypted in transit using certificates, key exchange methods and cipher suites rated "A" or "A+." Currently, that means an RSA 2048 bit key, using SHA256 with RSA, but ExaVault is continually reviewing best practices and updating their configuration to stay current. ExaVault's own privacy policy can be found here:

<https://www.exavault.com/privacy/>

Information accessed through or exchanged with DreamBox's site is encrypted in transit using certificates, key exchange methods and cipher suites rated "A" or "A+." Currently, that means an RSA 2048 bit key, using SHA256 with RSA, but DreamBox is continually reviewing best practices and updating our configuration to stay current.

Who Can Access Your Information

Only authorized employees, with a business need to handle your data, can access these protected network zones.

Those employees sign a binding agreement acknowledging that they will safeguard your privacy, and protect your data.

This agreement remains in force even if the employee leaves DreamBox Learning.

DreamBox conducts a background check on all employees, to confirm there is no criminal history or other disqualifying histories

We do not provide access to your data to 3rd parties, with these specific exceptions:

Limited data is shared with processing partners during registration or updates to registration information. For instance,

postal code, city, and state information are sent to a service to confirm an accurate postal code. Credit card processing is handled entirely external to DreamBox, by our partner Stripe.com. Stripe's privacy policy is found here: <https://stripe.com/privacy>

How and When We Remove Information

DreamBox retains information provided by the Customer ("Customer Data") only so long as we have a business-related need for it. We will destroy Customer-supplied data, as well as any other customer-identifying data, at any time upon request. However, our service is dependent upon the use of Customer-supplied Data, so destroying your data will mean you will no longer be able to use the DreamBox service. Derivative, anonymous data such as aggregate performance data will be retained.

Our Rules on Sharing Information

Except as provided in this Privacy Policy, DreamBox Learning WILL NOT disclose the information that it obtains from you to third parties without your express written permission, or where we believe, in good faith, that the law requires us to disclose the information. If you request that DreamBox share information provided by or collected from you (or in the case of School Customers, student users) directly with a third party designated by you, you agree that you (and not DreamBox) will be solely responsible for the use, storage, and maintenance of such information by such third party.

DreamBox Learning WILL NOT sell, trade, or assign any unaggregated personal information that it collects to third parties. We, however, may aggregate the information that we collect from users of our website to create demographic profiles and performance profiles regarding the progress of students who use the Programs. DreamBox Learning may share aggregated information with researchers, other clients, marketing professionals or potential investors. This aggregated information will be compiled and reported in the form of ANONYMOUS group statistics only in such a manner that makes individual student users unidentifiable.

In addition, DreamBox Learning may share information about the students, parents, legal guardians, and school officials that register to participate in the Programs, along with such registrants' Participation History, with contractual business partners of DreamBox Learning that are directly involved in the sale, distribution, operation, maintenance, and support of the Programs on behalf of DreamBox Learning. These partners function as an element of the DreamBox Programs, and do not have access to or use your information for any purpose other than providing the DreamBox Learning Programs.

If you request that DreamBox share any information provided by you (or in the case of School Customers, your student users) directly with a third party designated by you, then you agree that you (and not DreamBox) will be solely responsible for the use, storage, and maintenance of such information by such third party.

As DreamBox Learning continues to develop its business, it might sell some or all of its assets. In such transactions, customer information is generally one of the transferred business assets. An acquiring company would be required to protect all information that DreamBox Learning collects from users of our website and Programs in accordance with the terms of this Privacy Policy.

We Share Personal Information with these Third Parties
(none)

Currently, DreamBox does not disclose any information that it obtains from you to third parties. As noted above, we will share information with people and parties who already have the right to that information, who were the source of the information, or who you have requested and consented in writing that we share information with.

If this changes, we will update the list above with information about: (i) the third party, (ii) the types of information shared, (iii) the scope (which customers are affected), and (iv) the reasons for us sharing that information, including the third-parties use of that information.

Consenting to Our Collection and Use of Your Information

To use the DreamBox Programs, you will be asked to submit certain personal information about you and your student, and to authorize DreamBox Learning to use that information in a limited number of ways. If you are signing up directly as a parent or legal guardian of a student that will use DreamBox, we will require you to review and submit a Parental Consent as part of the registration process, which will require you to consent to our collection and use of information directly from your student over the Internet as described above. If you are the parent of a student using DreamBox through a school or district, your school will authorize our use of your information on your behalf.

Opting Out of Providing the Information We Request

Because the DreamBox Learning Programs are individualized and customized for each student, all the information we request from you and your student is required for you and your student to participate in the Programs, except for

certain information to be used for our communication purposes to you only. At any time, you may revoke your consent to allowing your student to participate in the DreamBox Learning Programs or refuse to allow DreamBox Learning to further use or collect your student's personal information. Any Anonymous Performance Data will be retained, but we will not retain any identifiable information regarding you or your student that you have provided. However, if you do any of the above, you and your student will not be able to participate in the Programs.

How You Can View, Change, or Remove Your Information

You can review and modify your Registration Information at any time by accessing our dashboard website using your login and password. You can also request that DreamBox remove your information: see "How to Contact Us" below for information on how to place a request.

How does DreamBox comply with Laws, Regulations, Industry Group Statements and other Guidelines

The core of our privacy policy is expressed in the "Privacy Statement" at the top of this page. The following items illustrate how this policy aligns with government regulations, industry standards and guidelines, technical standards, and third-party privacy pledges. We make frequent updates to this list. If you are looking for a standard that is not included here, please contact us with details.

US Federal regulations

CIPA (Children's Internet Protection Act)

The Children's Internet Protection Act (CIPA) is a federal law enacted by Congress in December 2000 to address concerns about access to offensive content over the Internet on school and library computers. CIPA imposes requirements on any school or library that receives funding support for Internet access or internal connections from the "E-rate" program — a program that makes certain technology more affordable for eligible schools and libraries. Our Programs do not provide links to external resources or chat rooms and do not contain any offensive or inappropriate material.

For more information about CIPA, please go to <https://www.fcc.gov/consumers/guides/childrens-internet-protection-act>.

COPPA (Children's Online Privacy Protection Act)

For our Individual Customers or parents or legal guardians of a student: Congress has enacted a law called the Children's Online Privacy Protection Act of 1998 (COPPA), designed to protect children's privacy during use of the Internet. DreamBox Learning has implemented practices consistent with the guidelines provided by the Federal Trade Commission to date. DreamBox Learning will never knowingly request, obtain, use, or disclose personally identifiable information or private content from anyone under the age of 13 without parental consent.

For our customers who are individuals, provided you are 18 years of age or older, you will be asked, at the time of registration, whether you consent to allowing users under the age of 13 to use your subscription and to be subject to this Privacy Policy. You must be the parent or legal guardian to grant such consent. If we receive this parental consent, we may receive personal information about children under the age of 13 listed on your subscription account in order to provide our Programs and services to them. **DREAMBOX LEARNING DOES NOT SHARE CHILDREN'S PERSONALLY IDENTIFIABLE INFORMATION WITH THIRD PARTIES.** If you are a parent or legal guardian of a user under 13 you may, at any time, revoke your consent to allow your student to use the Programs under your subscription, refuse to allow DreamBox Learning to further use or collect your student's personal information, or direct DreamBox Learning to delete all identifiable information regarding your student that you have provided. To do so, please contact our Privacy Officer at the contact information below. However, if you do any of the foregoing, your student will not be able to use the Programs.

For administrative officials of our School Customers, to the extent that DreamBox Learning collects, uses, or discloses personal information from children under the age of 13, it is done in strict accordance with this Privacy Policy and for the sole purpose of providing services to the School Customer and Individual Customer.

For more information about COPPA, visit the FTC site at <https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule> .

To report a COPPA violation, you can visit <https://www.ftccomplaintassistant.gov/#crnt&panel1-1> or call (877) FTC-HELP.

FERPA (The Family Educational Rights and Privacy Act)

For our School Customers: The Family Educational Rights and Privacy Act (FERPA) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. DreamBox Learning helps our School Customers be compliant with FERPA. Specifically:

Any sensitive online information is transmitted over secure channels

All student data are stored in ways that are not publicly accessible

Security audits are regularly performed to ensure data integrity

DreamBox Learning does not share information with third parties that could be used to identify students without consent from the student's parent, guardian, or school.

If a School Customer requests that student data be sent to a third party DreamBox Learning will:

send the data to the School Customer directly to transfer to the third party or

send the data directly to the third party designated by School Customer if requested by that customer, provided the School agrees that School Customer is solely responsible for use, storage, and maintenance of such information by such third party.

For more information about FERPA, please go to the US Department of Education site at <http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html>.

To report a FERPA violation, please visit <https://studentprivacy.ed.gov/file-a-complaint>.

HIPAA (Health Insurance Portability and Accountability Act)

Originally enacted in 1996, Health Insurance Portability and Accountability Act introduced most of the security and privacy guidelines now in place for US healthcare, as well as establishing guidelines for the insurance industry, guaranteeing interoperability of healthcare systems, and various other key reforms. In the context of education, the elements of HIPAA most likely to come into play are from HIPAA Title II (Administrative Simplification), particularly around Privacy, Security and Enforcement.

While HIPAA does not directly cover DreamBox's business or operations, as we are not a healthcare provider, insurance company, or healthcare information clearinghouse, some specific elements of HIPAA might be invoked in special circumstances. For instance, if a school or parent were to inadvertently share HIPAA-protected information with DreamBox, such as vaccination history or illness-related absence information, DreamBox would not be allowed to share that information, or utilize it for any purpose. Should HIPAA-protected information be inadvertently shared with us, DreamBox will notify the school or parent (as dictated by state law), and destroy the HIPAA-protected information.

In summary: DreamBox fully complies with HIPAA in all cases where it might apply, but HIPAA is not a direct guideline for DreamBox's security or privacy practices, being superseded by FERPA, COPPA, and other education and privacy laws.

For more information on HIPAA please refer to the US Dept of Health and Human Services site at <https://www.hhs.gov/hipaa/index.html>.

PPRA (Protection of Pupil Rights Amendments)

The Protection of Pupil Rights Amendments, originally established in 1978 and updated by the No Child Left Behind Act in 2001, says parents must first consent before a school (or their agent) may collect personal information from minor students as part of a survey, study, or evaluation. Personal information is defined to include things that are considered PII, as well as attitudes and opinions about sex, embarrassing personal history, and critical appraisals of family members.

In all cases, DreamBox complies with this law. DreamBox does not collect personal information directly from students. If a student submits or provides personal information of their own initiative – such as through an email or phone message – DreamBox quarantines that information from online systems, notifies the school or parent (as dictated by state law), and then removes the information. For more information about PPRA, visit the US Department of Education site at <https://www2.ed.gov/policy/gen/guid/fpco/ppra/parents.html>.

California regulations

CalOPPA (California Online Privacy Protection Act)

In 2004, California enacted a law that places certain requirements on all businesses collecting personal information from residents of California. Notably, this law requires the conspicuous posting of a clear, detailed privacy policy. It requires that companies comply with the elements of their privacy policy. It further specifies that privacy policies must contain this information:

CalOPPA Privacy Policy Requirement Found in these sections of our privacy policy

A list of the categories of personally identifiable information an operator collects

What information do we collect from you

What information do we collect from students

A list of the categories of third parties with whom an operator may share personally identifiable information

Who can access your information

A description of the process (if any) by which the consumer can review and request changes to his or her personally identifiable information as collected by an operator

How you can view, change, or remove your information

A description of the process by which the operator notifies consumers of material changes to an operator's privacy policy

How and when this privacy policy can change

The effective date of the privacy policy

Effective Date

AB1584 (2014)

Introduces concepts and language around third-party contractors for California School Districts. Clarifies that data remains the property of the school, not the contractor, and that should be reflected in contractual language. DreamBox is in full compliance with this law.

AB2097 (2016)

Covers collection of and handling of social security numbers. DreamBox does not collect, process or store Social Security Numbers.

CCPA (California Consumer Privacy Act)

For all our customers, parents, and students who are residents of California: The California Consumer Privacy Act (CCPA) is a California law that codifies some privacy and consumer rights. It was passed in 2018, and took effect on January 1, 2020. It guarantees that California residents have, among other rights,

The right to know what personal data any company has about them, where that data came from, and how it is used

The right to know whether their data is sold or disclosed, and to whom

The right to opt-out (prevent) the sale or disclosure of their data

The right to have their data deleted

CCPA provides some specific guidelines on how these rights will be protected and enabled by companies doing business with California residents.

DreamBox complies with all provisions of CCPA.

You can review your CCPA rights and place CCPA requests here. (Note – this link will take you away from the www.dreambox.com site.)

CPRA (California Privacy Rights Act)

Extends CCPA protections in many ways, including coverage of workplace information. DreamBox complies with all provisions of CPRA that are currently in effect, and will comply fully with the additional aspects of the law that take effect on January 1, 2022.

SOPIPA (Student Online Personal Information Protection Act)

California's SB-1177, often referred to as the Student Online Personal Information Protection Act (SOPIPA) forbids web sites and online service operators from knowingly selling, disclosing, using or allowing a 3rd party to use the personal information of a minor for marketing or advertising. It was enacted in 2016, and since that time, has been the model for laws in at least eight other states.

DreamBox fully complies with all aspects of SOPIPA and similar laws. We do not use individual or identifiable student personal information for marketing. We don't resell or share that information with third parties or allow them to reference that information for sales or marketing.

If you believe you have observed or experienced a SOPIPA violation, you should notify the office of the California Attorney General.

AB2799 (2016)

Clarifies and extends SOPIPA to explicitly provide protections to students and student data. Explicitly forbids creating or maintaining a marketing profile with student data. DreamBox is in full compliance with this law.

AB2828 (2016)

Extends existing regulations around data breaches and notification to cover cases where encryption keys have been or are believed to have been compromised or exposed. DreamBox is in full compliance with this law.

Other State and Municipal Regulations (See California separately, above)

Jurisdiction/Regulation DreamBox Response

Alabama: 8-38-1 – 8-38-12 (2018) Data Breach Notification Act DreamBox fully complies

Alaska: Sec. 45.48 Personal Information Protection Act DreamBox fully complies

Arizona:

Rev. Stat. 44-7601 Discarding and Disposing Of PII
SB1314 / Chpt. 180 Student Accountability System
DreamBox fully complies with each of these regulations
Arkansas:

Act 130 Personal Information Act updates
Act 1196 Student Online Personal Information Protection Act
DreamBox fully complies with each of these regulations
Colorado:

HB 16-1423 Student Data Transparency and Security Act
2021 Colorado Protection Act
DreamBox fully complies
Connecticut:

Act 16-189 Student Data Privacy Act
Act 17-200 Revisions to Student Data Privacy Act
Act 18-125 Revisions to Student Data Privacy Act
DreamBox fully complies with each of these regulations
Delaware:

Computer Security Breaches (Title 6, Sub II, Chap. 12B)
Delaware Online Privacy Protection Act (Title 6, Sub II, Chap. 12C)
Sb 79 / SB 208 Student Data Privacy Protection Act (Title 14, Chap.81A) – including required clauses CS1-B, CS1-C,
CS2, CS3, and CS4 of the Cloud Services Terms & Conditions
DreamBox fully complies with each of these regulations
Florida: Fla. Stat. 501.171(2) aka Florida Information Protection Act DreamBox fully complies
Georgia:

O.C.G.A. 10-1-910 – 912 Breach Notification
Executive Order (2013) on data sharing and data collection
O.C.G.A. 20-2-660 – 668 Student Data Privacy, Accessibility, And Transparency Act

DreamBox fully complies with each of these regulations
Hawaii:

H.A.R. 8-34 Education Rights and Privacy Of Students And Parents
SB 2607 (2016) Student Online Personal Information Protection Act

DreamBox fully complies with each of these regulations
Idaho: ID Code 28-51-105 Disclosure Of Breach DreamBox fully complies
Illinois:

815 ILCS 530/45 Personal Information Protection
Act 100-0315 (2017) Student Online Personal Protection Act
DreamBox fully complies with each of these regulations
Indiana:

Ind. Code 24-4.9-3-3.5 Disclosure Of Security Breach
Ind. Code 24-4-14 Customer Personal Information
DreamBox fully complies with each of these regulations
Iowa:

IA CODE 715C Personal Information Security Breach Protection
HF 2354 Student Privacy Protection
DreamBox fully complies with each of these regulations
Kansas:

K.S. 50-6,139b (supplement to Kansas Consumer Protection Act)
SB 367 Student Data Privacy Act
S Sub for HB2008 (2016) Student Online Personal Protection Act
DreamBox fully complies with each of these regulations
Kentucky:

KY REV STAT 365.732 Breach Notification

KY REV STAT 61.932 Breach Investigation Procedures
KY REV STAT 365.734 Student Data And Cloud Computing
DreamBox fully complies with each of these regulations
Louisiana:

Database Security Breach Notification (SB205 Act 499) & Act 382 (2018)
La. Rev. Stat. 51:3074 (2018 S.B. 361)
HB 946 / HB 1076 (2014)
HB 718 (2015)
DreamBox fully complies with each of these regulations
Maine:

SP 183 Student Information Privacy Act
LD 1616
DreamBox fully complies with each of these regulations
Maryland:

Personal Information Protection Act (14-3501), including amendments through HB 974 (2018)
HB 298 Student Data Privacy Act of 2015
DreamBox fully complies with each of these regulations
Massachusetts:

General Law Ch. 93H Security Breaches
General Law Ch. 93I Data Destruction
201 CMR 17.00 Data collection limitations and requirements for 3rd-party processors
603 CMR 23.00 STUDENT RECORDS
DreamBox fully complies with each of these regulations
Michigan:

SB 33 2016
SB 510 2016 Student Online Personal Protection Act
DreamBox complies with all relevant clauses.
Minnesota: Chapter 325M (Internet Privacy and Service Providers)
[NOTE: this does not directly apply to providers like DreamBox, only to ISPs] DreamBox complies with all relevant clauses.
Mississippi: MISS. CODE ANN. 75-24-29 & REV STAT 407.1500 Breach Notification DreamBox fully complies
Missouri: MO REV STAT 407.1500 Breach Notification DreamBox fully complies
Montana:

MONT. CODE ANN. 30-14-1701– 1705 Breach Notification
HB 745 Montana Pupil Online Personal Information Protection Act
DreamBox fully complies with each of these regulations
Nebraska:

LB 512 Student Online Personal Protection Act
AB 7 Definitions and Clarifications
DreamBox fully complies with each of these regulations
Nevada:

SB 463 (2015)
AB 221 (2015)
Nev. Rev. Stat. Section 603A
SB 403
SB 220 Data Handling and Notification Requirements for Providers
DreamBox full complies with each of these regulations. Required disclosures are included in this Privacy Policy
New Hampshire:

HB 1587 (2014) collection and disclosure of student data
HB 322 (2015) protection of personally-identifiable data
HB 520 (2015) privacy protections for student online personal information
HB 1612 (2018) data security in schools
DreamBox fully complies with each of these regulations
New Jersey: N.J. REV. STAT. 56:8-161 – 166 Personal Information DreamBox complies with all relevant clauses.
New Mexico: 2017 H.B. 15, Chap. 36 : Data Breach DreamBox fully complies
New York:

AB 8556 (2014) inc. Student Bill of Rights
SHIELD Act (2020) covers data breaches and other privacy issues
DreamBox fully complies with each of these regulations
North Carolina:

SB 815 (2014) – portions about data transparency
HB 632 (2015) Act to Protect Student Online Privacy
DreamBox fully complies with each of these regulations
North Dakota: N.D. CENT. CODE 51-30-01 – 07 Breach Notification DreamBox fully complies
Ohio:

OHIO REV. CODE 1354.01 Data Protection Act
OHIO REV. CODE 1349.19 Breach Notification
DreamBox fully complies with each of these regulations
Oklahoma:

24 O.S. 24-161 – 166 Breach Notification
HB 1989 The Student Data Accessibility, Transparency & Accountability Act
DreamBox fully complies with each of these regulations
Oregon:

OAR 581-021-0220 – 0440 Student Education Records (relevant sections)
SB 684 (ORS 646) Personal Information and Breach Notification
SB 187(ORS 646.607 and 646.605) Student Information Protection Act
DreamBox fully complies with each of these regulations
Pennsylvania:

73 PA. STAT. 2301 – 2308 Breach Notification
2016 HB 1606 Data Collection Reduction
DreamBox fully complies with each of these regulations
Rhode Island: Title 11, Chap. 11-49.3 (Identity Theft Protection Act) DreamBox fully complies
South Carolina:

Title 39, Section 39-1-90 (Breach notification)
Title 37, Chapter 20, section 37-20-190 (Data Destruction)
Title 59, Chapter 1, Section 59-1-490 (Education Data Use)
DreamBox fully complies with each of these regulations
South Dakota: S.D. CODIFIED LAWS 22-40-19 – 26 Breach Notification DreamBox fully complies
Tennessee:

HB 1549 & 49-1-708 Student Data Accessibility, Transparency & Accountability Act
HB 1931 (2015) Student Online Personal Protection Act
SB 1835 On Commercial Use and Disclosure of Student Data
DreamBox fully complies with each of these regulations
Texas:

HB 2087 SOPIPA
TX B&C Code 521.053 Breach Notification
DreamBox fully complies with each of these regulations
Utah:

Utah Code 13-44 Protection of Personal Information Act
HB 163 Data Breach Guidance
HB 358 / Utah Code 53E-9-308 Student Data Protection Act
SB 102 Privacy Training and other Requirements
SB 163/SB 207 Updates to Student Data Protection Act
DreamBox fully complies with each of these regulations
Vermont: Title 9, Chap. 62 (Protection of Personal Information inc. Breach Notification) DreamBox fully complies
Virginia:

HB 1612 (2015) Omnibus student privacy law
HB 519 (2016) Data disclosure and transparency
HB 749 & HB 750 (2016) Updated student data privacy law
SB 951 (2017) Parent access to data

HB 1 (2018) as amended by HB 2449 (2019) Parent rights and opt-out
Title 18.2-186.6 Breach Notification
VA CDPA Omnibus privacy law protecting all Virginia consumers. Similar in scope to California's CCPA.
DreamBox fully complies with each of these regulations
Washington:

Title 19.255 Breach Notification
Title 19.215 Disposal of Information
SB 5419 / Title 28A.604 Student Privacy
Title 28A.605 Parental Rights
DreamBox fully complies with each of these regulations
Washington D.C.: B21-0578 – Protecting Students Digital Privacy Act of 2016 DreamBox fully complies
West Virginia:

HB 4316 (2014) Student Data Accessibility, Transparency, and Accountability Act
HB 4261 (2016) updates to Student Data Accessibility, Transparency, and Accountability Act
W. VA. CODE 46A-2A-101 – 105 Breach Notification
DreamBox fully complies with each of these regulations
Wyoming:

SF 79 Provider security and data handling responsibilities
W.S. 40-12-501 and 40-12-502 (Breach Notifications), including amendments S.F. 35 and S.F. 36 (2015)
HB 0008 (2017) Student data privacy, security, and transparency
HB 0009 (2017) Student ownership and privacy rights
DreamBox fully complies with each of these regulations

European regulations
GDPR

The European Union's (EU) General Data Protection Regulation (GDPR) is a comprehensive privacy and security law that governs how companies of all sizes must behave when handling, storing, transmitting and removing the personal data of individuals who are residing in the EU. DreamBox does not currently market to customers or intentionally perform business activities in the EU. However, we are working to align our privacy policy and practices to be in compliance with the overall principles and restrictions of GDPR.

GDPR provides guidelines on necessary components of a Privacy Policy. Below is that list, with DreamBox's information or response, included for each. Again, DreamBox is not currently operating in or marketing to residents of the EU, but we are working to align our policies with GDPR principles, and we are providing this information for customers concerned about the issues raised by GDPR and similar pending legislation in other jurisdictions:

GDPR Privacy Policy Requirement DreamBox response

The identity and contact details of the organization, its representative, and its Data Protection Officer
In this policy, see:

Who we are and what we do

How to contact us

The purpose and legal basis for the organization to process an individual's personal data

In this policy, see:

Why we have your information

What information do we collect from you

The legitimate interests of the organization In general, DreamBox data uses are under the "consent" exceptions of GDPR, but we may obtain and use your data in some specific instances under the "legitimate interests" exception, for exigent circumstances such as Investigating possible security violations

Any recipient or categories of recipients of an individual's data All personal information provided by individual customers and school customers is received through automated processes and interfaces into systems administered by the Site Reliability Engineering (SRE) Team of DreamBox Learning, Inc.

Details regarding transfer of personal data to any country outside the EU, and the safeguards taken with that data

DreamBox data is stored and processed in the United States. Details on the protection of that data is found in several sections of this policy.

The retention period or criteria used to determine the retention period of the data DreamBox retains your data as long as there is a business need for this data, to allow us to provide the educational service we've contracted to provide.

The existence of each data subject's rights

Right to Information

Right of Access

Right of Redress
Right of Removal
Right of Restriction
Right to Data Portability
Right to Object
Rights concerning automated processing
In this policy, see:

How to contact us
Why we have your information
What information do we collect from you
Opting out of providing the information we request
How you can view, change, or remove your information
DreamBox does not provide any reports or extract relevant to the “Data Portability” right.

The right to withdraw consent at any time
In this policy, see:

Opting out of providing the information we request
The right to lodge a complaint with a supervisory authority In this policy, see the sections for individual regulations, such as FERPA, COPPA, and SOPIPA.
The categories of personal data obtained
In this policy, see:

What information do we collect from you
What information do we collect from students
The existence of an automated decision-making system, including profiling, and information about the significance, set up, and consequences of this system DreamBox does not employ any automated decision-making systems that leverage or refer to personal data. The DreamBox system does employ automated decision-making systems that rely on responses and inputs from students during completion of lessons.

Industry Groups, Pledges, and Statements
Student Privacy Pledge

The Future of Privacy Forum (FPF) and The Software & Information Industry Association (SIIA) put together a statement of principles that they believe should be endorsed by every responsible company that collects, handles or stores student personal information. DreamBox is a long-standing signatory of that pledge, and we fully endorse its overall principles and individual elements. The pledge is structured as a set of commitments, covering specific actions a company will or won't do; for example, we affirm that:

We will not collect, maintain, use or share student personal information beyond that needed for authorized educational purposes, or as authorized by the parent/student

We will not sell student personal information

We will not knowingly retain student personal information beyond the time period required to support the authorized educational purposes, or as authorized by the parent/student

We will not build a personal profile of a student for marketing or any purpose other than for supporting authorized educational/school purposes, or as authorized by the parent/student

We will maintain a comprehensive security program that is reasonably designed to protect the security, privacy, confidentiality, and integrity of student personal information against risks

We will disclose clearly in contracts or privacy policies, including in a manner easy for parents to find and understand, what types of student PII we collect, if any, and the purposes for which the information we maintain is used or shared with third parties

We will require that our vendors with whom Student PII is shared in order to deliver the educational service, if any, are obligated to follow these same commitments for the given Student PII

We will incorporate privacy and security when developing or improving our educational products, tools, and services and comply with applicable laws

The full Student Privacy Pledge is here: <https://studentprivacypledge.org/privacy-pledge-2-0/> .

Answers to common questions about the pledge: <https://studentprivacypledge.org/faqs/> .

Please contact DreamBox (see “How to contact us” below) if you believe we are not fully complying with the Student Privacy Pledge.

Software and Technical Standards

Cookies

As a standard practice, DreamBox Learning uses “cookies.” A cookie is a small amount of data sent to your browser from our web server and stored on your computer, then sent back to the server by your browser each time you access our website. Cookies are used solely for the required operations of our website and services. We do not use cookies to collect any personal information, nor do we use them for behavioral advertising, to build a student profile unrelated to the use of DreamBox, or for any other reason. Please note that if you refuse the DreamBox Learning cookie (by turning cookies off in your browser or by clicking “don’t accept” if you have set your browser to warn you before accepting cookies), our Programs will not work. Cookies cannot be used to gather personal information from your computer.

Do Not Track (DNT signals)

In response to an FTC privacy report in 2010, the major browser manufacturers implemented a feature called “Do Not Track” or simply, “DNT.” The idea was that, by enabling DNT signals in your browser configuration, you would tell sites and services that they were not allowed to track your movements, responses, and choices.

There is no legal obligation for any company to honor these DNT signals. Also, there is no clear guidance or common understanding of what DNT means for collecting information necessary to operate a site. Because of the lack of clarity and usable best practice information, DreamBox does not currently respond to or interact with DNT signals. We will continue to evaluate DNT as a technology and may consider a change to this policy in the future.

How to Contact Us

Our Data Privacy Officer is J.B. Krewson, VP of Security and IT. If you have any questions about your privacy or security measures at DreamBox Learning, please contact:

privacy@dreambox.com

Or call our security hotline at

1-888-867-2750

Or, you can contact us through our primary location and main phone number:

DreamBox Learning, Inc.
777 108th Ave NE, Suite 2300
Bellevue, WA 98004
(425) 637-8900

How to contact other sources and authorities about privacy issues

US Federal Government – Protecting Your Privacy:

<https://www.usa.gov/privacy> (general)

<https://tech.ed.gov/privacy/> (From the Office of Educational Technology)

Federal Trade Commission – Protecting Your Child’s Privacy Online: <https://www.consumer.ftc.gov/articles/0031-protecting-your-childs-privacy-online>

How and when this privacy policy can change

DreamBox updates this privacy policy at least annually, and whenever we need to express changes to business practices or to clarify how we address a specific law, policy, or technical issue.

When we make significant updates to this policy, we will notify all customers whose data we currently hold. We will also prominently display information about the change on our primary information website, <https://www.dreambox.com>. We will generally not send direct notification for additions to reference lists and items: state standards, or links to government and third-party sites providing supporting information.

