



CONTRACT ADDENDUM

Protection of Student Personally Identifiable Information

1. Applicability of This Addendum

The Wayne-Finger Lakes BOCES/EduTech) and Desmos, Inc. (“Vendor”) are parties to a contract dated 9/21/2021 (“the underlying contract”) governing the terms under which BOCES accesses, and Vendor provides, grade 6 - 8 curriculum (“Product”). Wayne-Finger Lakes BOCES/EduTech use of the Product results in Vendor receiving student personally identifiable information as defined in New York Education Law Section 2-d and this Addendum. The terms of this Addendum shall amend and modify the underlying contract and shall have precedence over terms set forth in the underlying contract and any online Terms of Use or Service published by Vendor.

2. Definitions

- 2.1. “Protected Information”, as applied to student data, means “personally identifiable information” as defined in 34 CFR Section 99.3 implementing the Family Educational Rights and Privacy Act (FERPA) where that information is received by Vendor from BOCES or is created by the Vendor’s product or service in the course of being used by BOCES.
- 2.2. “Vendor” means Desmos, Inc..
- 2.3. “Educational Agency” means a school BOCES, board of cooperative educational services, school, or the New York State Education Department; and for purposes of this Contract specifically includes Wayne-Finger Lakes BOCES/EduTech.
- 2.4. “BOCES” means the Wayne-Finger Lakes BOCES/EduTech.
- 2.5. “Parent” means a parent, legal guardian, or person in parental relation to a Student.
- 2.6. “Student” means any person attending or seeking to enroll in an educational agency.
- 2.7. “Eligible Student” means a student eighteen years or older.
- 2.8. “Assignee” and “Subcontractor” shall each mean any person or entity that receives, stores, or processes Protected Information covered by this Contract from Vendor for the purpose of enabling or assisting Vendor to deliver the product or services covered by this Contract.
- 2.9. “This Contract” means the underlying contract as modified by this Addendum.

3. Vendor Status

Vendor acknowledges that for purposes of New York State Education Law Section 2-d it is a third-party contractor, and that for purposes of any Protected Information that constitutes education records under the Family Educational Rights and Privacy Act (FERPA) it is a school official with a legitimate educational interest in the educational records.

4. Confidentiality of Protected Information

Vendor agrees that the confidentiality of Protected Information that it receives, processes, or stores will be handled in accordance with all state and federal laws that protect the confidentiality of Protected Information, and in accordance with the BOCES Policy on Data Security and Privacy, a copy of which is Attachment B to this Addendum.



5. Vendor Employee Training

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

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

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

7. Ownership and Location of Protected Information

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

7.2. BOCES may request access to the BOCES's Protected Information at all times through the term of this Contract. BOCES may request Vendor export Protected Information in piecemeal or in its entirety at their discretion, and Vendor shall comply.

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

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

8. Purpose for Sharing Protected Information

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

9. Downstream Protections

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



10. Protected Information and Contract Termination

- 10.1. The expiration date of this Contract is defined by the underlying contract.
- 10.2. Upon expiration of this Contract without a successor agreement in place, Vendor shall assist BOCES in exporting all Protected Information previously received from, or then owned by, BOCES.
- 10.3. Vendor shall thereafter securely delete and overwrite any and all Protected Information remaining in the possession of Vendor or its assignees or subcontractors (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies of shared data) as well as any and all Protected Information maintained on behalf of Vendor in secure data center facilities.
- 10.4. Vendor shall ensure that no copy, summary or extract of the Protected Information or any related work papers are retained on any storage medium whatsoever by Vendor, its subcontractors or assignees, or the aforementioned secure data center facilities.
- 10.5. To the extent that Vendor and/or its subcontractors or assignees may continue to be in possession of any de-identified data (data that has had all direct and indirect identifiers removed) derived from Protected Information, they agree not to attempt to re-identify de-identified data
- 10.6. Upon request, Vendor and/or its subcontractors or assignees will provide a certification to BOCES from an appropriate officer that the requirements of this paragraph have been satisfied in full.

11. Data Subject Request to Amend Protected Information

- 11.1. In the event that a parent, student, or eligible student wishes to challenge the accuracy of Protected Information that qualifies as student data for purposes of Education Law Section 2-d, that challenge shall be processed through the procedures provided by the BOCES for amendment of education records under the Family Educational Rights and Privacy Act (FERPA).
- 11.2. Vendor will cooperate with BOCES in retrieving and revising Protected Information, but shall not be responsible for responding directly to the data subject.

12. Vendor Data Security and Privacy Plan

- 12.1. Vendor agrees that for the life of this Contract the Vendor will maintain the administrative, technical, and physical safeguards described in the Data Security and Privacy Plan set forth in Attachment C to this Contract and made a part of this Contract.
- 12.2. Vendor warrants that the conditions, measures, and practices described in the Vendor's Data Security and Privacy Plan:
- 12.3. align with the NIST Cybersecurity Framework 1.0;
- 12.4. equal industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection;
- 12.5. outline how the Vendor will implement all state, federal, and local data security and privacy contract requirements over the life of the contract, consistent with the BOCES data security and privacy policy (Attachment B);
- 12.6. specify the administrative, operational and technical safeguards and practices it has in place to protect Protected Information that it will receive under this Contract;
- 12.7. demonstrate that it complies with the requirements of Section 121.3(c) of this Part;
- 12.8. specify how officers or employees of the Vendor and its assignees who have access to Protected Information receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;



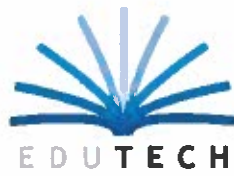
- 12.9. specify if the Vendor will utilize sub-contractors and how it will manage those relationships and contracts to ensure Protected Information is protected;
- 12.10. specify how the Vendor will manage data security and privacy incidents that implicate Protected Information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify BOCES; and
- 12.11. describe whether, how and when data will be returned to BOCES, transitioned to a successor contractor, at BOCES's option and direction, deleted or destroyed by the Vendor when the contract is terminated or expires.

13. Additional Vendor Responsibilities

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

- 13.1 Vendor shall limit internal access to Protected Information to those individuals and Assignees or subcontractors that need access to provide the contracted services;
- 13.2 Vendor will not use Protected Information for any purpose other than those explicitly authorized in this Contract;
- 13.3 Vendor will not disclose any Protected Information to any party who is not an authorized representative of the Vendor using the information to carry out Vendor's obligations under this Contract or to the BOCES unless (1) Vendor has the prior written consent of the parent or eligible student to disclose the information to that party, or (ii) the disclosure is required by statute or court order, and notice of the disclosure is provided to BOCES no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order;
- 13.4 Vendor will maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Protected Information in its custody;
- 13.5 Vendor will use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the secretary of the U.S. Department of HHS in guidance issued under P.L. 111-5, Section 13402(H)(2);
- 13.6 Vendor will notify the BOCES of any breach of security resulting in an unauthorized release of student data by the Vendor or its Assignees in violation of state or federal law, or of contractual obligations relating to data privacy and security in the most expedient way possible and without unreasonable delay but no more than seven calendar days after the discovery of the breach; and

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



Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

Signatures

For Wayne-Finger Lakes BOCES/EduTech

For Desmos, Inc.

[Handwritten Signature]
Date

[Handwritten Signature]
Date

9/21/21

9/21/2021



Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

Attachment A – Parent Bill of Rights for Data Security and Privacy

Wayne-Finger Lakes BOCES (EduTech)

Parents' Bill of Rights for Data Privacy and Security

The Wayne-Finger Lakes BOCES (EduTech) seeks to use current technology, including electronic storage, retrieval, and analysis of information about students' education experience in the BOCES, to enhance the opportunities for learning and to increase the efficiency of our BOCES and school operations.

The Wayne-Finger Lakes BOCES (EduTech) seeks to insure that parents have information about how the BOCES stores, retrieves, and uses information about students, and to meet all legal requirements for maintaining the privacy and security of protected student data and protected principal and teacher data, including Section 2-d of the New York State Education Law.

To further these goals, the Wayne-Finger Lakes BOCES (EduTech) has posted this Parents' Bill of Rights for Data Privacy and Security.

1. A student's personally identifiable information cannot be sold or released for any commercial purposes.
2. Parents have the right to inspect and review the complete contents of their child's education record. The procedures for exercising this right can be found in Board Policy 5500 entitled Family Educational Rights and Privacy Act (FERPA).
3. State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.
4. A complete list of all student data elements collected by the State is available at <http://www.nysed.gov/data-privacy-security/student-data-inventory> and a copy may be obtained by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.
5. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to the Chief Privacy Officer, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.


Revised October 2019

Signatures

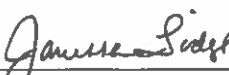
For Wayne-Finger Lakes BOCES/EduTech

For Desmos, Inc.

Date


9/21/21

Date 9/21/2021


Date 9/21/2021



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

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

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

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

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

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

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

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

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

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



- b) Personally Identifiable Information, as applied to student data, means 40 personally identifiable information as defined in section 99.3 of Title 34 of the Code of 41 Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 42 U.S.C 1232-g, and as applied to teacher and principal data, means personally 43 identifying information as such term is defined in Education Law §3012-c(10).
- c) Breach means the unauthorized access, use, or disclosure of student data 9 and/or teacher or principal data. Good faith acquisition of personal information by an employee or agent of the BOCES for the purposes of the BOCES is not a breach of the security of the system, provided that private information is not used or subject to unauthorized disclosure.

Notification Requirements Methods of Notification

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

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

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

In the event that any residents are to be notified, the BOCES shall notify the New York State Chief Privacy Officer, the New York State Cyber Incident Response Team, the office of Homeland Security, and New York State Chief Security Officer as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected residents.

The Superintendent or his/her designee will establish and communicate procedures for parents, eligible students, and employees to file complaints about breaches or unauthorized releases of student, teacher or principal data (as set forth in 8 NYCRR §121.4). The Superintendent is also authorized to promulgate any and all other regulations necessary and proper to implement this policy.

Data Protection Officer

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



Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

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

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

Annual Data Privacy and Security Training

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

References:

Education Law §2-d

8 NYCRR §121

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

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



Attachment C – Vendor’s Data Security and Privacy Plan

The Wayne-Finger Lakes BOCES Parents Bill of Rights for Data Privacy and Security, which is included as Attachment B to this Addendum, is incorporated into and make a part of this Data Security and Privacy Plan.

(Vendor can attached)

Privacy Policy

Desmos, Inc. (“we” or “Desmos”) is committed to protecting your privacy. This Privacy Policy describes our collection and use of personal information collected from visitors to our website and our mobile application(s) (collectively, our “Service”), including the Service offered at www.desmos.com, teacher.desmos.com, student.desmos.com and any other website, app, or online service which links to this Privacy Policy. “You” or “your” means a visitor or a user (whether logged in or not) of our Service.

A note about Student Data: Our Desmos Service may be used by schools, school districts, or teachers (collectively referred to as “Schools”) in a classroom setting. When Desmos contracts with a School to provide the Service through student.desmos.com to students in a classroom (“Students”), we may have access to Student Data (defined below). This Privacy Policy does not govern our access to Student Data. We consider Student Data to be highly confidential and our use of Student Data is governed by our agreements with the schools. Please see our Student Data Privacy Statement for information about how we collect and use Student Data gathered during the provision of the Desmos Service to Schools.

This Privacy Policy is incorporated into and is subject to our Terms of Service, which governs your use of the Desmos Services.

1. Information Collected

a. Personal Data. You can use the Service without registering for an account or providing any other personal data. If you create an account on the Desmos Services, or communicate with Desmos, you may provide to Desmos certain information by which someone could personally identify you, such as your name, email or unique username (“Personally Identifiable Information”), as well as information about yourself such as your employment or level of schooling by which someone could not personally identify you (“Demographic Information”). When we link Demographic Information to your Personally Identifiable Information, we treat all of it as Personally Identifiable. We also collect information when you save or post content to the Service (“User Content”), authorize us to access your device camera and photo roll, and communicate with us. We refer to all of this data collectively as “Personal Data”. We may also collect Personal Data about you from a third party Internet site or service. For example, if you login to your Desmos account through Google or another authentication tool, or if you interact with Desmos on social media, we may collect the Personal Data you authorize that third party service to share.

b. Usage Data. We automatically collect certain technical usage information when you use the Desmos Services (“Usage Data”). Usage Data includes the information that your web browser or mobile application automatically sends to our servers whenever you visit. The Usage Data collected in our logs may include information such as your web request, Internet Protocol address, operating system, browser type, browser language, referring / exit pages and URLs, platform type, click history, domain names, landing pages, pages viewed and the order of those pages, the amount of time spent on particular pages, the date and time of your request, and whether you opened an email. Typically, this information is collected through log files, web beacons, browser cookies, or other device

disable cookies on certain mobile devices and/or certain browsers. For more information on cookies, visit www.allaboutcookies.org. Remember, some features of the Desmos Services may not function properly if cookies or mobile device identifiers are not enabled. In addition, the Desmos Services may use third party analytics and bug tracking software (including, without limitation, Google Analytics and Bugsnag) to collect further Usage Data regarding the online usage patterns of our users and bugs in our Services. We may combine Usage Data with Personal Data in a manner that enables us to trace Usage Data to an individual user. Although we do our best to honor the privacy preferences of our visitors, we are not able to respond to Do Not Track signals from your browser at this time. We do not permit third party advertising networks or other third parties to collect information about your browsing behavior from our website for advertising purposes.

2. Use of Your Information

a. Use. We use your Personal Data and Usage Data (together, “User Information”) to operate, maintain, and provide to you the features and functionality of the Desmos Services and for related business purposes. We may use your User Information to (a) improve the quality and design of the Desmos Services and to create new features and services by storing, tracking, and analyzing user preferences; (b) remember information so that you will not have to re-enter it during your visit or the next time you use the Desmos Services; (c) provide custom, personalized content and information; (d) monitor aggregate metrics such as total number of visitors, pages viewed, etc.; and (e) diagnose and fix technology problems and otherwise plan for and enhance our Service. Desmos may provide personalized content and information to our users, including teachers, school administration officials, and other users associated with Schools. However, Desmos shall never use Student Data to engage in targeted advertising, nor shall Desmos direct advertising to student users on student.desmos.com, nor shall Desmos ever use any third-party advertising network on any Desmos Service.

b. Communications Preferences. We will not use your email address or other Personally Identifiable Information to send you marketing messages unless you provide your consent, or as part of a specific program or feature for which you will have the ability to opt-out. You can always opt-out of receiving promotional email from us by clicking on the “unsubscribe” feature at the bottom of each email or by adjusting your email subscription preferences in your settings. We may, however, use your email address without further consent for non-marketing or administrative purposes, such as notifying you of important Desmos Services changes or for customer service purposes.

3. Disclosure of Your Information

a. Your Publication. You may, by using applicable sections of the Desmos Services (including sections which enable you to create graphs, perform lessons, provide comments, upload video and pictures), share your User Information, including Personally Identifiable Information and other content that you create or post to others accessing the Desmos Services. Please see the Student Data Privacy Statement to learn how Student Data may be shared.

b. Service Providers. We share User Information with our trusted third party service providers and other individuals who perform services on our behalf, for example, providing customer service support, hosting services, analytics and other services we utilize to help us provide our Service or conduct our business. These service providers access and use User Information only to provide services to Desmos under reasonable confidentiality terms.

c. Partners. At your direction, we may provide your User Information to our partners (“Partners”) that are integrated with the Desmos Network. For example, we may share certain User Information when you login to the Desmos Services using Google login and similar authentication tools. We may also share User Information when we provide the Service with a Partner, such as when we work with a school or educational institution to provide the Service to students. Please see our Student Data Privacy Statement to learn more about how student data may be shared. User Information that is shared with a third party Partner may be subject to that Partner’s privacy and data security policies. We are not responsible for the content or privacy and security practices and policies of the Partners. We encourage you to learn about our Partners’ privacy and security policies before providing them with your User Information or directing us to provide them with your User Information.

d. Other Required Sharing. We may share User Information: (i) if required to do so by law, or in the good-faith belief that such action is in compliance with state and federal laws (including, without limitation, copyright laws) or in response to a court order, subpoena, legal process or search warrant, or (ii) if we believe, in good faith, such action is appropriate or necessary to enforce our Terms of Service, to exercise our legal rights, to take precautions against liability, to investigate and defend ourselves against any claims or allegations, to assist government enforcement agencies, to protect the security or integrity of the Desmos Services, and to protect the rights, property, or personal safety of Desmos, Education Providers, our users or third parties.

e. School Collaboration. For Schools utilizing our School Collaboration functionality, school administration officials and teachers (collectively, "Admins") may be able to share information, resources, and materials through the School Collaboration Features. Depending on School's use of various features of the Service, an Admin may be able to share information with other Admins and/or invite other Admins to access, review, and edit School material. Sharing functionality will be determined by the School settings.

f. Sharing of Student Work. In some instances, Student Data, including, for example, student's response to a prompt, (collectively, "Student Work") may be visible to other students in the same classroom. A teacher or school administration official will be able to monitor any such Student Work and will be able to hide it at their discretion, for example if said Student Work is in violation of a school's policies or the teacher's desired classroom culture.

g. Merger or Sale. If we merge, sell, or otherwise transfer all or a portion of our business, we will not transfer your Personally Identifiable Information without first giving you the ability to opt-out of the transfer, unless the new owner intends to maintain and provide the applicable Desmos Services as a going concern, and provided that the new owner has agreed to data privacy standards no less stringent than our own. We may also transfer personal information – under the same conditions – in the course of mergers, acquisitions, bankruptcies, dissolutions, reorganizations, liquidations, similar transactions or proceedings involving all or a portion of our business.

4. Your Choices

You may decline to submit Personally Identifiable Information through the Desmos Services, in which case Desmos or your School may not be able to provide certain Desmos Services to you. You may update or correct your name, email address, or password at any time by visiting your "Account Settings" link. You may also delete your account altogether there. With respect to User Information provided by your School, please reach out to your School to request removal or updates of such information. If you have any questions about reviewing, modifying, or deleting your information, or if you want to remove your name or comments from our website or publicly displayed content, you can contact us directly at support@desmos.com. We may not be able to modify or delete your information in all circumstances.

5. Data Security

We care about the security of your information and employ physical, administrative, and technological safeguards designed to preserve the integrity and security of all information collected through our Service. Access to information is limited (through user/password credentials and, in some cases, two factor authentication) to those employees who require it to perform their job functions. We use industry standard SSL (secure socket layer technology) encryption to transfer personal information. Other security safeguards include but are not limited to data encryption, firewalls, physical access controls to buildings and files, and employee training. You can help protect against unauthorized access to your account and personal information by selecting and protecting your password appropriately and limiting access to your computer and browser by signing off after you have finished accessing your account.

6. Children's Privacy

Our Service is not directed to children under 13, unless and until a School has provided consent and authorization for a student under 13 to use the Service and for Desmos to collect information from such student. If you believe that we have inadvertently collected Personal Data from a child under 13 years of age without parental consent, then please alert us at support@desmos.com and we will promptly delete the child's Personal Data from our systems.

7. For Our International Users

By using this Service, you consent to the transfer of your personal information to the United States and to the processing of your personal information in the United States in accordance with this Privacy Policy. You understand that your personal information will be subject to the laws of the United States, which may be different from those of your country of residence.

8. Contact Us

Please feel free to contact us with any questions or comments about this Privacy Policy, your personal information, your consent, or your opt-in or opt-out choices as follows:

Desmos, Inc.

ATTN: Privacy Agent

9450 SW Gemini Drive, PMB 49136

Beaverton, OR 97008

Email: support@desmos.com

9. Changes and Updates

a. Updates. This Privacy Policy may be revised periodically and this will be reflected in the "date last modified" set forth below. Your continued use of the Desmos Services following such update constitutes your agreement to the revised Privacy Policy. You can see the history of the changes to this Privacy Policy [here](#).

b. Last Modified. This Privacy Policy was last modified June 20, 2020.

