RCSD ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

Vendor Statement of Compliance
Data Privacy and Protection

This agreement is entered into between the Roseville City School District ("LEA" or "District") and Amplify Education, Inc. ("Service Provider") on 01/05/2024 ("Effective Date").

WHEREAS, the LEA and the Service Provider entered into an agreement for Educational Technology services;

WHEREAS, the LEA is a California public entity subject to all state and federal laws governing education, including but not limited to California Assembly Bill 1584 ("AB 1584"), the California Education Code, the Children's Online Privacy and Protection Act ("COPPA"), and the Family Educational Rights and Privacy Act ("FERPA");

WHEREAS, AB 1584 requires, in part, that any agreement entered into, renewed or amended after January 1, 2015, between a local education agency and a third-party service provider must include certain terms;

NOW, THEREFORE, the Parties agree as follows:

Section I: General - All Data

1. **PASSWORD SECURITY.** All passwords are considered secure. Vendors may not disseminate any passwords unless specifically directed by Educational or Technology Services management. Vendors will not provide information concerning Admin accounts (ROOT Admin, container Admin, local NT administrator or Domain administrator) or their equivalent to any persons. District personnel ONLY will disseminate this information. Vendors will never create "back door" or "generic" user accounts on any systems unless specifically directed to do so by LEA management.

   Agree: Yes ◉ No ○

2. **SYSTEM SECURITY.** Unauthorized access to or modification of District systems including file servers, routers, switches, NDS and Internet services is prohibited. Any attempt to bypass or subvert any District security system, both hardware, and software is prohibited.

   Agree: Yes ◉ No ○

3. **PRIVACY**. The vendor will adhere to all provisions of the Federal Family Educational Rights and Privacy Act (FERPA, 20 U.S.C. 123g), California Education Code and district policies regarding the protection and confidentiality of data. At all times, the vendor will consider all data collected in the course of their duties to be protected and confidential. Release of this data can only be authorized by Technology & Information Services management and state and federal law.

   Agree: Yes ◉ No ○

ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

Section I: General - All Data *(Continued)*

4. **REUSE**: Vendors shall not copy, duplicate, sell, repackage or use for demonstration purposes any Roseville City School District data without the prior, written consent of Educational or Technology Services management.

   Agree: Yes ◉ No ○

5. **TRANSPORT**: Vendor must provide a secure channel (S/FTP, HTTPS, SSH, VPN, etc) for the District to "push" data to the vendor and to extract data as required. Vendors will not have direct access to District systems and will not "pull" data at any time.

   Agree: Yes ◉ No ○

6. **EXTERNAL SECURITY:** Vendor must attach to this document reasonable evidence that their system is secure from external hacking and attacks. Devices such as firewalls and technologies such as NAT are the minimum requirements. Active IDS or similar technology is preferred.

   Agree: Yes ◉ No ○

7. **INTERNAL SECURITY:** Vendors must attach to this document reasonable evidence that their system is secure from internal hacking and attacks. Describe the interactions vendor personal (or their representatives) will have directly with District data. How is uploaded data from the District handled and processed? Who has access to this data? What happens to the data after the upload is complete? What security safeguards are in place to protected unauthorized access to District data? How are backup performed and who has access to and custody of the backup media? How long are backup maintained; what happens to the District data once the backup is "expired"? If any data is printed, what happens to these hard copy records?

   Agree: Yes ◉ No ○

8. **DISTRICT ACCESS:** Vendor must provide a secure means (see Item 5 above) for the District to extract ALL data from the vendor system. This can either be an online extraction tool or a vendor-provided extract as needed by the District (not to exceed quarterly). Describe the means and format of the data (delimited, Excel, MDB, SQL Dump).

   Agree: Yes ◉ No ○

9. **TERMINATION:** Upon termination of this agreement as provided herein, the vendor will permanently delete all customer data from their system as allowed by state and federal law. Vendor may be required to certify the destruction of LEA data within 90 days of contract termination.

   Agree: Yes ◉ No ○

ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

Section II: AB1584 Compliance - Student Information Only

1. Vendor agrees that the Roseville City School District retains ownership and control of all student data.
   Agree: Yes (●) No ( )

2. Vendor must attach to this document a description of how student-created content can be exported and/or transferred to a personal account.
   Agree: Yes (●) No ( )

3. Vendor is prohibited from allowing third-parties access to student information beyond those purposes defined in the contract.
   Agree: Yes (●) No ( )

4. Vendor must attach to this document a description of how parents, legal guardians and students can review and correct their personally identifiable information.
   Agree: Yes (●) No ( )

5. Vendor will attach to this document evidence how student data is kept secure and confidential.
   Agree: Yes (●) No ( )

6. Vendor will attach to this document a description of procedures for notifying affected parents, legal guardians or eligible students when there is an unauthorized disclosure of student records.
   Agree: Yes (●) No ( )

7. Vendor certifies that student records will not be retained or available to a third party once the contract has expired or is canceled (See Page 2, Item 9).
   Agree: Yes (●) No ( )

8. Vendor will attach to this document a description of how they and any third party affiliates comply with FERPA.
   Agree: Yes (●) No ( )

9. Vendor and its agents or third parties are prohibited from using personally identifiable information from student records to target advertising to students
   Agree: Yes (●) No ( )

RCSD ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

Section III: SB 1177 SOPIPA Compliance - Student Information Only

1. Vendors cannot target advertising on their website or any other website using information acquired from students.
   Agree: Yes (●) No ( )

2. Vendors cannot create a profile for a student except for school purposes as defined in the executed contract.
   Agree: Yes (●) No ( )

3. Vendors cannot sell student information.
   Agree: Yes (●) No ( )

4. Vendors cannot disclose student information unless for legal, regulatory, judicial, safety or operational improvement reasons.
   Agree: Yes (●) No ( )

5. Vendors must attach to this document evidence of how student information is protected through reasonable security procedures and practices.
   Agree: Yes (●) No ( )

6. Vendors must delete district-controlled student information when requested by the District.
   Agree: Yes (●) No ( )

7. Vendors must disclose student information when required by law, for legitimate research purposes and for school purposes to educational agencies.
   Agree: Yes (●) No ( )

As an authorized representative of my organization, I accept the conditions listed in this document.

Alexandra Walsh
Print Name

Alexandra Walsh 01 / 08 / 2024
Signature, Date

Laura Assem
Print Name (Roseville City School District)

01/09/2024
Signature, Date (Roseville City School District)

ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

EXHIBITS

Section 1.6: External Security
Please see attached EXHIBITS document

Section 1.7: Internal Security
Please see attached EXHIBITS document

Section II.2: Exporting of Student-Created Content
Please see attached EXHIBITS document

Section II.4: Review and Correcting Personally Identifiable Information (PII)
Please see attached EXHIBITS document

ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

EXHIBITS

Section II.5: Securing Student Data
Please see attached EXHIBITS document

Section II.6: Disclosure Notification
Please see attached EXHIBITS document

Section II.8: Family Educational Rights and Privacy Act (FERPA) Compliance
Please see attached EXHIBITS document

Section III.5: How Student Data is Protected:
Please see attached EXHIBITS document

EXHIBITS

This Exhibit is hereby attached to the Vendor Statement of Compliance Data Privacy and Protection. In the event of any conflict between the Vendor Statement of Compliance Data Privacy and Protection and the information provided in this attached Exhibit, this Exhibit shall govern. For sake of clarity, the agreement for Educational Technology services shall incorporate the terms and conditions located at https://amplify.com/customer-terms and this Exhibit.

Section I.3: Privacy

For sake of clarity, Vendor's compliance with district policies will be limited to what is provided to Vendor in advance or otherwise outlined herein. In addition, the data protection obligations will apply to personally identifiable information.

Section I.4: Reuse

For sake of clarity, the district's written consent shall only be required for the use of data that identifies the district or an individual.

Section I.6: External Security

As a provider of technology solutions to schools, Amplify's commitment to data privacy and security is essential to our organization. As described at https://amplify.com/security, Amplify maintains a comprehensive information security program based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the NIST SP 800-53 Rev. 5 family of information security controls. These provide a robust framework of best practices from which an organization can build its security policies and protocols based on identified risks, compliance requirements, and business needs. They cover critical practice areas, including access control, configuration management, incident response, security training, and other information security domains.

Endpoint security

Access to production systems at Amplify is restricted to a limited set of internal Amplify users to support technical infrastructure, troubleshoot customer issues, or other purposes authorized by the district. In addition, Amplify requires multi-factor (MFA) authentication methods for access to all production systems. MFA involves a combination of something only the user knows and something only the user can access. For example, MFA for administrative access could involve entering a password as well as entering a one-time passcode sent via text message to the administrator's mobile phone. The use of MFA reduces the possibility that an unauthorized individual could use a compromised password to access a system.

Infrastructure security

Network filtering technologies are used to ensure that production environments with student data are properly segmented from the rest of the network. Production environments only have limited external access to enable customers to use our web interfaces and other services. In addition, Amplify uses firewalls to ensure that development servers have no access to production environments.

Other measures that Amplify takes to secure its operational environment include system monitoring to detect anomalous activity that could indicate potential attacks and breaches.

Monitoring

Intrusion detection and prevention systems (IDS/IPS) are in place to analyze the network device logs, monitor the network and report anomalous activity for appropriate resolution.

For sake of clarity, this provides reasonable evidence that Vendor has implemented appropriate security measures in its system designed to secure such systems from external hacking.

For more, see https://amplify.com/security

Section I.7: Internal Security

Access control

Amplify's access control principles dictate that all student data we store on behalf of customers is only accessible to district-authorized users and to a limited set of internal Amplify users who may only access the data for purposes authorized by the district. Districts maintain control over their internal users and may grant or revoke access.

In limited circumstances and strictly for the purposes of supporting school districts and maintaining the functionality of systems, certain Amplify users may access Amplify systems with student data. All such access to student data by Amplify technicians or customer support requires both authentication and authorization to view the information.

Encryption

Data encryption is an important element of our protection of sensitive data at rest and in transit, and is reviewed and updated as appropriate annually, based on the latest standards and guidelines published by OWASP and NIST.

In transit: Amplify encrypts all student data in transit over public connections, using Transport Layer Security (TLS), commonly known as SSL, using industry-standard protocols, ciphers, algorithms, and key sizes.
At rest: Amplify encrypts student data at rest using the industry-standard AES-256 encryption algorithm.

Building the right roles into applications

Permissions within Amplify applications are designed on the principle that school districts control access to all student data. To facilitate this, Amplify applications are designed so that roles and permissions flow from the district to the individual user. For example, applications that offer schools a way to collect and report on assessment results have a web interface that requires district administrators to authorize individuals to view student data.

Security controls within applications are used to ensure that the desired privacy protections are technically enforced within the system. For example, if a principal is supposed to see only the data related to his or her school, Amplify ensures that, throughout the design and development process, our products restrict principals from seeing records for any students outside his or her school.

To make sure Amplify applications properly enforce permissions and roles, our development teams conduct reviews early in the design process to ensure roles and permissions are an essential component of the design of new applications.

Building security controls into applications

Amplify applications are also developed to minimize security vulnerabilities and ensure industry-standard application security controls are in place.

As part of the development process, Amplify has a set of application security standards that all applications handling student data are required to follow, including:

Student data is secured using industry standard encryption when in transit between end-users and Amplify systems.
Applications are built with password brute-force attack prevention.
User sessions expire after a fixed period of time.
We also conduct manual and automated static code analysis as well as dynamic application security testing to preemptively identify vulnerabilities published by industry leaders such as OWASP (Open Web Application Security Project)

Backups

Amplify backs up student data on a continuing basis to Amazon's Simple Storage Service. Backups are tested regularly. Backups are encrypted at rest and securely deleted on a regular basis. Data backups are stored within production environments, with access restricted to a limited set of internal Amplify users to support technical infrastructure, troubleshoot customer issues, or other purposes authorized by the district. Personally identifiable information in backups is encrypted using the industry-standard AES-256 encryption algorithm. Backups are regularly destroyed on appropriate schedules.

Describe the interactions vendor personal (or their representatives) will have directly with District data. How is uploaded data from the District handled and processed? Who has access to this data? What happens to the data after the upload is complete? What security safeguards are in place to protected unauthorized access to District data? How are backup performed and who has access to and custody of the backup media? How long are backup maintained; what happens to the District data once the backup is "expired"? If any data is printed, what happens to these hard copy records?

Data destruction
Upon notice from our school customers, Amplify will return, delete, or destroy student personally identifiable data stored by Amplify in accordance with applicable law and customer requirements. Unless otherwise notified by our school customer, we will delete or de-identify student PII after termination of our Agreement with the customer.

Student Data is disposed or de-identified in accordance with applicable law and customer requirements, aligned to guidance including NIST IR 8053, HIPAA Privacy Rule 164.514(a), and NIST SP 800-88 rev 1.

Amplify will certify data deletion or destruction upon customer request.

For sake of clarity, this provides reasonable evidence that Vendor has implemented appropriate security measures in its system designed to secure such system from internal hacking.

Section I.8 District Access

For sake of clarity, this access shall be limited to personally identifiable data or other data as mutually agreed to by the parties.

Section I.9: Termination

For sake of clarity, deletion upon termination will only be applicable to personally identifiable information in customer data.

Section II.2: Exporting of Student-Created Content

Amplify partners with customers to help meet their data reporting goals. Administrative users can download detailed student-level data in CSV format. Upon request, Amplify can arrange for regular delivery (via secure file transfer or API) of student performance and usage data. Amplify has deep experience with major charter networks, large districts, and multiple states in data delivery and integration.

Section II.3: This party access to information

For sake of clarity, third parties will be prohibited from accessing personally identifiable information beyond the purposes outlined in the contract.

Section II.4: Review and Correcting Personally Identifiable Information (PII)

See attached Amplify Customer Privacy Policy.

FERPA requires schools to provide parents with access to their children's education records, and parents may request that the school correct records that they believe to be inaccurate or misleading. If you are a parent or guardian and would like to review, correct, or update your child's data stored in our Products, contact your School District. Amplify will work with your School District to enable your access to and, if applicable, correction of your child's education records.

Section II.5: Securing Student Data

See attached Amplify Customer Privacy Policy.

Amplify maintains a comprehensive information security program and uses industry standard administrative, technical, operational, and physical measures to safeguard Student Data in its possession against loss, theft and unauthorized use, disclosure, or modification. Amplify performs periodic risk assessments of its information security program and prioritizes the remediation of identified security vulnerabilities. Please see amplify.com/security for a detailed description of Amplify's security program.

Section II.6: Disclosure Notification

See attached Amplify Customer Privacy Policy.

In the event Amplify discovers or is notified that Student Data within our possession or control was disclosed to, or acquired by, an unauthorized party, we will investigate the incident, take steps to mitigate the potential impact, and notify the School Customer in accordance with Applicable Laws.

For sake of clarity, notification obligations shall apply in the event there is unauthorized disclosure of personally identifiable information in student records. In addition, as the owner of the student records, the District shall be responsible for the timing and content of the notices to be sent. The District will be responsible for providing notice directly to individuals whose personal information was affected and Amplify will provide reasonable assistance to help the District meet it's legally required notification obligations..

Section II.7 Access to student records upon contract expiration

For sake of clarity, this section is limited to personally identifiable information in student records.

Section II.8: Family Educational Rights and Privacy Act (FERPA) Compliance

See attached Amplify Customer Privacy Policy.

Section III.1 No targeted advertising

For sake of clarity, Vendor will not use personally identifiable student information for targeted advertising.

Section III.4: Disclosure of student information

For sake of clarity, Vendor may disclose data, including personally identifiable student information, to the extent necessary to deliver the Services in accordance with the contract and applicable law. See attached Amplify Customer Privacy Policy.

Section III.5: How Student Data is Protected:

See attached Amplify Customer Privacy Policy and amplify.com/security for a detailed description of Amplify's security program.

Update 6/30/2023: This Privacy Policy has been updated to address new state law data privacy requirements.

We advise you to read this Privacy Policy in its entirety, including the jurisdiction-specific provisions in the appendix. Our Notice At Collection for California residents is available in the Notice for our California Customers.

Customer Privacy Policy: K–12 Schools

Who We Are:

Amplify Education, Inc. ("**Amplify**") is leading the way in next-generation curriculum and assessment. Amplify's programs provide teachers with powerful tools that help them understand and respond to the needs of each student and use data in a way that is safe, secure, and effective.

Our Products and Services:

Amplify's products support classroom instruction and learning and include Amplify CKLA, Amplify ELA, Amplify Science, Amplify Desmos Math, Desmos Math, Boost Reading, Boost Math, mCLASS, Mathigon, services at teacher.desmos.com (for creating and assigning activities) and student.desmos.com (for use of the activities or curricula as directed by an instructors), and any other product or service that links to this Privacy Policy (together, the "**Products**").

Our Products are primarily geared towards K–12 students, educators, and staff who use the Products pursuant to an agreement or with the permission of School Districts and State Agencies ("**Authorized School Users**"). We also provide limited opportunities for teens and parents on behalf of children under 13 ("**Child Users**") to sign up for an account for at-home use of our Products. See the Appendix for additional information for users of our at-home use of our Products.

What This Privacy Policy Covers:

This Customer Privacy Policy ("**Privacy Policy**") describes how Amplify collects, uses, and discloses personal information through the provision of Products.

For purposes of this Privacy Policy, "**you**" and "**your**" means Authorized Users.

For additional information that applies to the Product(s) that are designed for home use, visit the Appendix–Supplemental Disclosures of this Privacy Policy.

This Privacy Policy does not apply to Amplify's handling of:

- information collected from users of Amplify's company website, which is governed by our Website Privacy Policy.
- applicant data that we process in accordance with our applicant privacy notice.

There may be different contractual terms or privacy policies in place with some of our School Customers. Such other terms or policies may supersede this Privacy Policy for information collected or released under those terms. If you have any questions as to which legal agreement or privacy policy controls the collection and use of your personal information, please contact us using the information provided below. Unless expressly superseded, this Privacy Policy is incorporated into and is subject to the Agreement that governs your use of the Products.

Our Approach to Student Data Privacy: In the course of providing the Products to our School Customers and their Authorized School Users, Amplify collects, receives, generates, or has access to **"Student Data**,**"** which is information that directly relates to an identifiable student.

We consider Student Data to be confidential and we collect and use Student Data solely for educational purposes in connection with providing our Products to, or on behalf of, our School Customers, as described in this Privacy Policy and our Agreements. We work to maintain the security and confidentiality of Student Data that we collect or store, and we enable our School Customers to control the use, access, sharing, and retention of Student Data.

Our collection and use of Student Data is governed by our Agreements with our School Customers, including this Privacy Policy, and applicable laws which may include the federal Family Educational Rights and Privacy Act of 1974 ("**FERPA**"), the Children's Online Privacy Protection Act ("**COPPA**"), the Protection of Pupil Rights Amendment ("**PPRA**"), as well as other applicable federal, state, and local privacy laws and regulations ("**Applicable Laws**"). With respect to FERPA, Amplify receives Student Data as a "school official" under Section 99.31 of FERPA for the purpose of providing its Products, and such Student Data is owned and controlled by the School Customer.

Amplify is also an early adopter and proud signatory of the Student Privacy Pledge, an industry-wide pledge to safeguard privacy and security of Student Data.

1. Definitions

Capitalized terms not defined in this section or above will have the meaning set forth by Applicable Laws.

"Agreement" means the underlying contractual agreement between Amplify and the School Customer.

"**Authorized Users**" means all authorized users of our Products, including Authorized School Users, parents and legal guardians, and children under the age of 13 who are permitted to sign up for our Products only with verifiable consent from their parent or guardian.

"Authorized School Users" means K–12 students, educators, and staff using Amplify's Products pursuant to an Agreement or with the permission of the School District or State Agency.

"School Customer" means the School District or State Agency that is the party to the Agreement to provide the Amplify Products to the School Customer's Authorized School Users.

"School District" means a local education agency, school network, independent school, or other regional education system.

"State Agency" means the educational agency primarily responsible for the supervision of public elementary and secondary schools in any of the 50 states, the Commonwealth of Puerto Rico, the District of Columbia, or other territories and possessions of the United States, as well as a national or regional ministry or department of education in other countries, as applicable.

2. What Personal Information Do We Collect?

When you access or use our Products, you may choose to provide us with personal information, including Student Data. This information may be provided to us directly (e.g. when an account is created or through communications with us) or through our Products.

Student Data. Below is a list of the categories of Student Data that may be collected by Amplify or its Products, either directly or through the School Customer's use of the various features and configurations of the Products:

- **Identifier and Enrollment Data,** such as name, email, school / state ID number, username and password, grade level, homeroom, courses, teacher names.
    - **Why?** Most of Amplify's Products require some basic information about who is in a classroom and who teaches the class—student or teacher Identifier and Enrollment data. This information is provided to Amplify by our School Customers, either directly from the School Customer's student information system or via a third party with whom the School Customer contracts to provide that information.
- **Demographic Data**, such as date of birth, socioeconomic status, race, national origin, and preferred or primary language.
    - **Why?** To support school instructional and reporting requirements, Amplify's Products allow School Customers to view reports and analyze data using student demographic and other special indicators. For example, a School District may wish to analyze student literacy assessment results based on English Language Learner status to better tailor classroom instruction, and in that case may provide the associated indicator as part of the enrollment information to enable that reporting.
- **School Records**, such as grades, attendance, assessment results, and Individualized Education Plan status (i.e. whether a plan is in place)
    - **Why?** Some of our Products support grading assignments and administering formative, diagnostic, and curriculum-based assessments. Teachers use that data to support students' progress in the program or help with instructional decisions. We do not collect specific details from an IEP, nor do we collect health or other sensitive information.
- **Schoolwork and Student Generated Content**, which includes any information contained in student assignments and assessments, including information in response to instructional activities and participation in collaborative or interactive features of our Products, such as student responses to academic questions and student-written essays, as well as images, video, and audio recordings.

- **Why?** As part of the digital learning experience, some of our Products may enable students to write texts and create and upload images, video, and audio recordings. For example, in Amplify ELA, students may write essays or submit short-form responses in our platform as part of a lesson on literature. As another example, in Boost Reading, student interactions with reading skills games are recorded to keep track of the student's progress to level up in the program and to provide visibility to teachers on how students are mastering the skills.

- **Teacher Comments and Feedback**, such as scores, written comments, or other feedback that educators may provide about student responses or student course performance.

    - **Why?** To enable teachers to track the performance and provide feedback to their students.

Other Data. We may collect the following types of personal information from all other Authorized Users:

- **Contact Information**, such as name and email address, as well as grade level taught, school name and school location, whether you are a teacher, administrator, or other authorized person that creates an account or uses our Products or communicates with us.

- **Account Information**, such as customer user login and password, for account creation and access purposes.

- **Survey Responses**, which you provide in response to surveys or questionnaires.

- **Device and Usage Data.** Depending on the Product, we may collect certain information about the device used to connect to our Product, such as device type and model, browser configurations, and persistent identifiers, such as IP addresses and unique device identifiers. We may collect device diagnostic information, such as battery level, usage logs, and error logs, as well as usage, viewing, and technical information (e.g., email open rates), such as the number of requests a device makes, to ensure proper system capacity for all Authorized Users. We may collect IP addresses and use that information to approximate device location to support operation of the Product. To the extent that we collect this information from website visitors who have not signed up for an account, this data is solely used to support operation of the Product and is not linked to Student Data.

    - **How? Cookies and Similar Technologies.** We collect device and usage data through "cookies," Web beacons, HTML5 local storage, and other similar technologies, which are used in some of our Products.

    - **Why?** We use this information to remember returning users and facilitate ease of login, to customize the function and appearance of the Products, and to improve the learning experience. This information also helps us track product usage for various purposes, including website optimization, to ensure proper system capacity, troubleshoot and fix errors, provide technical assistance and customer support, provide and monitor the effectiveness of our Products, monitor and address security concerns, and compile analytics for product improvement and other internal purposes. Learn how to opt out of cookies and similar technologies

by reading the "What Rights and Choices Do You Have?" section of this Privacy Policy below.

3. How Do We Use Personal Information?

Student Data. Amplify uses Student Data for educational purposes, to provide the Products, and to ensure secure and effective operation of our Products, including:

- to provide and improve our educational Products;
- to support School Customers' and Authorized School Users' activities;
- to ensure secure and effective operation of our Products;
- for purposes requested or authorized by the School Customer or Authorized School User or as otherwise permitted by Applicable Laws;
- for adaptive or personalized learning purposes, provided that Student Data is not disclosed to third parties;
- for customer support purposes, to respond to the inquiries and fulfill the requests of our School Customers and their Authorized School Users;
- to enforce Product access and security controls; and
- to conduct system audits and improve protections against the misuse of our Products, or to detect and prevent fraud and other harmful activities.

We also use personal information to power the adaptive and personalized learning features of the Products. For example, we may make instructional recommendations to teachers and students based on the student's progress in the program. These recommendations are offered as optional, additional learning support.

Other Data. Amplify may use Authorized User information for the purposes for which Student Data is used as set forth above. Amplify does not use Student Data for marketing purposes, but it may use the personal information of other Authorized Users for marketing in limited circumstances (e.g. to periodically send newsletters and other promotional materials), and as otherwise required or permitted, or as we may notify you at the time of collection. Learn how to opt out of these communications by reading the "What Rights and Choices Do You Have?" section of this Privacy Policy below.

Amplify may use aggregate or de-identified data as described in the Aggregate/De-identified Data section below.

4. To Whom Do We Disclose Personal Information?

Student Data. We disclose Student Data to third parties only as needed to provide the Products under the Agreement, as directed or permitted by the School Customer or Authorized School User, and as required by law. Such disclosures may include but are not limited to the following:

- to other Authorized School Users of the School Customer entitled to access such data in connection with the Products;

- to our service providers, subprocessors, or vendors who have a legitimate need to access such data in order to assist us in providing or supporting our Products, such as platform, infrastructure, and application software. We contractually bind such parties to protect Student Data in a manner consistent with those practices set forth in this Privacy Policy and in accordance with Applicable Laws. List of Amplify subprocessors is available at http://www.amplify.com/subprocessors;

- to comply with the law, respond to requests in legal or government enforcement proceedings (such as complying with a subpoena), protect our rights in a legal dispute, or seek assistance of law enforcement in the event of a threat to our rights, security, or property or that of our affiliates, customers, Authorized Users, or others;

- in the event Amplify or all or part of its assets are acquired or transferred to another party, including in connection with any bankruptcy or similar proceedings, provided that successor entity will be required to comply with the privacy protections in this Privacy Policy with respect to information collected under this Privacy Policy, or we will provide the School Customer with notice and an opportunity to opt out of the transfer of such data prior to the transfer; and

- except as restricted by Applicable Laws or contracts with our School Customers, we may also share Student Data with Amplify's affiliated education companies, provided that such disclosure is solely for the purposes of providing Products and at all times is subject to this Policy.

Other Data. Amplify discloses Authorized User information for the purposes for which Student Data is used as set forth above. Amplify may also disclose Authorized User information as otherwise required or permitted, or as disclosed at the time of collection.

5. Aggregate/De-identified Data

Amplify may use de-identified or aggregate data for purposes allowed under FERPA and other Applicable Laws, to research, develop, and improve educational sites, services, and applications and to demonstrate the effectiveness of the Amplify Products. Amplify will not attempt to re-identify de-identified data. We may use aggregate information (which is information that has been collected in summary form such that the data cannot be associated with any individual) for analytics and reports. For example, our marketing materials may note the total number of students served by our programs in the prior year, but that information cannot be used to identify any one student. We may also share de-identified or aggregate data with research partners to help us analyze the information for product improvement and development purposes.

Records and information are de-identified when all personal information has been removed or obscured, such that the remaining information does not reasonably identify a specific individual. We de-identify Student Data in compliance with Applicable Laws and in accordance with the guidelines of NIST SP 800-122. Amplify has implemented internal procedures and controls to protect against the re-identification of de-identified Student Data. Amplify does not disclose de-identified data to its research partners unless that party has agreed in writing not to attempt to re-identify such data.

6. Data Prohibitions, Advertising, Advertising Limitations

Amplify will not:

- sell Student Data to third parties;
- use or disclose Student Data to inform, influence, or enable targeted advertising to a student based on Student Data or information or data inferred over time from the student's usage of the Products;
- use Student Data to develop a profile of a student for any purpose other than providing the Products to a School Customer or Authorized School User, or as authorized by a parent or legal guardian;
- use Student Data for any commercial purpose other than to provide the Products to the School Customer or Authorized School User, or as permitted by Applicable Laws.

Amplify may, from time to time, provide customized content, advertising, and commercial messages to Authorized Users, provided that such advertisements shall not be based on Student Data or directed to K–12 students. Amplify may use de-identified Student Data to recommend educational products or services to School Customers and their Authorized Users (subject to exceptions permitted under applicable law), or to notify such users about new educational product updates, features, or services.

7. External Third-Party Services

This Privacy Policy applies solely to Amplify's Products and practices. Amplify School Customers and other Authorized Users may choose to connect or use our Products in conjunction with third-party services and Products. Additionally, our sites and Products may contain social media plugins (e.g. like or share buttons) as well as links to third-party websites or services. This Privacy Policy does not address, and Amplify is not responsible for, the privacy, information, or other practices of such third parties. Customers should carefully consider which third-party applications to include among the Products and services they provide to students and vet the privacy and data security standards of those providers.

Authorized Users may be able to log in to our Products using third-party sign-in services such as Clever or Google. These services authenticate your identity and provide you with the option to share certain personal information with us, including your name and email address, to pre-populate our account sign-up form. If you choose to enable a third party to share your third-party account credentials with Amplify, we may obtain personal information via that mechanism. You may configure your accounts on these third-party platform services to control what information they share.

8. Security

Amplify's servers are hosted, managed, and controlled by us in the United States and are not intended to subject Amplify to the laws or jurisdiction of any jurisdiction other than that of the United States. If you are located outside the United States, you understand and consent to having Student Data collected and maintained by Amplify processed in the United States. United States

data protection and other relevant laws may not be the same as those in your jurisdiction. This includes the use of cookies and other tracking technologies as described herein. See also Notice for European Economic Area and United Kingdom Customers below.

Student Data

Amplify maintains a comprehensive information security program and uses industry standard administrative, technical, operational, and physical measures to safeguard Student Data in its possession against loss, theft and unauthorized use, disclosure, or modification. Amplify performs periodic risk assessments of its information security program and prioritizes the remediation of identified security vulnerabilities. Please see amplify.com/security for a detailed description of Amplify's security program.

In the event Amplify discovers or is notified that Student Data within our possession or control was disclosed to, or acquired by, an unauthorized party, we will investigate the incident, take steps to mitigate the potential impact, and notify the School Customer in accordance with Applicable Laws.

Other Data

Outside of Student Data, Amplify uses commercially reasonable administrative, technical, personnel, and physical measures to safeguard personal information in its possession against loss, theft, and unauthorized use, disclosure or modification.

9. What Rights and Choices Do You Have?

What Choices Do You Have?

Opt-out of Marketing Communications. If you want to stop receiving promotional materials from Amplify, you can email us at privacy@amplify.com or follow the unsubscribe instructions at the bottom of each email.

Opt-out of Cookies and Similar Tracking Technologies. With respect to cookies, you may be able to reject cookies through your browser or device controls. Note that you have to opt-out of cookies on each browser or device that you use. If you replace, change, or upgrade your browser or device, or delete your cookies, you may need to use these opt-out tools again. Please be aware that disabling cookies may negatively impact your experience as some features may not work properly. To learn more about browser cookies, including how to manage or delete them, check the "Help," "Tools," or similar section of your browser.

What Rights Do You Have With Respect to Student Data?

Review and Correction. FERPA requires schools to provide parents with access to their children's education records, and parents may request that the school correct records that they believe to be inaccurate or misleading.

- If you are a parent or guardian and would like to review, correct, or update your child's data stored in our Products, contact your School District. Amplify will work with your

School District to enable your access to and, if applicable, correction of your child's education records.

- If you have any questions about whom to contact or other questions about your child's data, you may contact us using the information provided below.

No third-party website tracking. Amplify does not track students across third-party websites and does not respond to Do Not Track (DNT) signals. Amplify does not permit third-party advertising networks to collect information from or about students using Amplify educational Products for the purpose of serving targeted advertising across websites and over time and Amplify will never use Student Data for targeted advertising.

What is our Deletion/Retention Policy?

Upon request, we provide the School Customer the opportunity to review and delete the personal information collected from students.

Student Data Retention. We will retain Student Data for the period necessary to fulfill the purposes outlined in this Privacy Policy and our Agreement with the School Customer. We do not knowingly retain Student Data beyond the time period required to support a School Customer's or Authorized School User's educational purpose, unless authorized by the School Customer or Authorized School User. Upon request, Amplify will return, delete, or destroy Student Data stored by Amplify in accordance with applicable law and customer requirements. We may not be able to delete all data in all circumstances, such as information retained in technical support records, customer service records, back-ups, and similar business records. Unless otherwise notified by our School Customer, we will delete or de-identify Student Data after termination of our Agreement with the School Customer.

10. COPPA

Except as described in the Appendix, we do not knowingly collect personal information from a Child User unless and until a School Customer or educator has, on behalf of a parent or guardian, authorized us to collect such information to provide the Products. We comply with all applicable provisions of COPPA. To the extent COPPA applies to the information we collect, we process such information for educational purposes only, at the direction of the partnering School District or State Agency and on the basis of educational institutional consent. If you are a parent or guardian and have questions about your child's use of the Products and any personal information collected, please direct these questions to your child's school.

11. Updates to This Privacy Policy

We may change this Privacy Policy in the future. For example, we may update it to comply with new laws or regulations, to conform to industry best practices, or to reflect changes in our product offerings. When these changes do not reflect material changes in our practices with respect to use and/or disclosure of Authorized Users' personal information, including Student Data, such changes to the Privacy Policy will become effective when we post the revised Privacy Policy on our website. In the event there are material changes in our practices that would result in Authorized Users' personal information being used in a materially different manner than was disclosed when the information was collected, with respect to Student Data, we will notify

the School Customer, and with respect to other information, we will notify you via email and provide an opportunity to opt out before such changes take effect.

12. Contact Us

If you have questions about this Privacy Policy, please contact us at:

Email: privacy@amplify.com
Mail: Amplify Education, Inc.
55 Washington St.#800
Brooklyn, NY, 11201
Phone: (800) 823-1969
Attn: General Counsel

To report a security vulnerability, visit https://amplify.com/report-a-vulnerability/.

Appendix – Supplemental Disclosures

1. Notice for Parents/Guardians Regarding Mathigon

While our Products are primarily geared towards School Customers, we do provide an opportunity for children and teens to sign up for a Mathigon account at home—outside of the school context—only with verifiable parental consent from parents or guardians if their child is a Child User.

Please note that most parts of Mathigon can be used without creating an account or providing any personal information that directly identifies you. However, if you are a parent or guardian and would like to authorize your child to sign up for a Mathigon account so that we can offer personalized educational services (e.g. by remembering your child's progress, tailoring our content to your child's interests or abilities, or suggesting what to learn next), please read our Acceptable Use Policy, available at amplify.com/acceptable-use, which explains our verifiable consent process, and then sign up by visiting https://mathigon.org/signup.

What Rights Do You Have? If you are the parent or guardian of a Child User, you may request that we provide for your review, delete from our records, or cease collecting any personal information from your Child User. To exercise these rights, please contact us by sending an email to: help@amplify.com. You may also be able to correct your personal information provided to us, download a copy of all the personal information we have about you, or delete your account via your account settings page. Please note that we may retain certain information as permitted by law. We may also retain cached or archived copies of the information we collect for a certain period of time.

2. Notice for our California Customers

Personal Information We Collect	How We Use Personal Information
Student Data, which includes: ● Roster Information ● Demographic Data, such as race and national origin ● School Records ● Account Information	● To provide and improve our educational Products; ● To support School Customers' and Authorized School Users' activities; ● To ensure secure and effective operation of our Products;

• Schoolwork and Student Generated Content • Teacher Comments and Feedback • Device and Usage Data	• For purposes requested or authorized by the School Customer or Authorized School Users, or as otherwise permitted by Applicable Laws; • For adaptive or personalized learning purposes, provided that Student Data is not disclosed; • For customer support purposes, to respond to the inquiries and fulfill the requests of our School Customers and their Authorized School Users; • To enforce product access and security controls; and • To conduct system audits and improve protections against the misuse of our Products, or to detect and prevent fraud and other harmful activities.
Authorized Users, which includes: • Contact Information • Account Information • Survey Responses • Device and Usage Data	• For the purposes for which Student Data is used as set forth above; • For marketing purposes in limited circumstances (e.g. to periodically send newsletters and other promotional materials), which will not be based on Student Data or directed to K–12 students • As otherwise required or permitted, or as we may notify you at the time of collection.

We do not sell or share your personal information, as described in California law.

We retain your personal information for as long as reasonably necessary for the purposes disclosed in the chart above. Additional information about our retention of Student Data can be found in Section 9 of this Privacy Policy.

Please see the Additional U.S. State Privacy Law Rights section of this appendix for information about your rights pursuant to applicable California law.

Notice of Financial Incentive

As part of our services, there will be opportunities to complete surveys and questionnaires. As an incentive for completing the survey or questionnaire, you can voluntarily provide personal information as an entry into a raffle drawing or to obtain other benefits, discounts, offers, or deals that may constitute a financial incentive under California law ("**Financial Incentive**"). The categories of personal information required for us to provide the Financial Incentives include: contact information and any other information that you choose to provide when you complete the survey.

Participation is voluntary and you can opt out at any time before the survey is complete. We do not allow students to participate in our surveys.

The value of the personal information we collect in connection with our Financial Incentives is equivalent to the value of the benefit offered.

3. Notice for other U.S. Customers—Additional U.S. State Privacy Law Rights

You have the following rights, where provided under applicable state law, regarding your personal information (each of which is subject to various exceptions and limitations):

- **Access.** You have the right to request, up to two times every 12 months, that we disclose to you the categories of personal information collected about you; the categories of sources from which the personal information is collected; the categories of personal information sold or shared; the business or commercial purpose for collecting, selling, or sharing the personal information; the categories of third parties with whom personal information was shared; and the specific pieces of personal information collected about you.

- **Correction.** You have the right to request that we correct inaccurate personal information collected from you, subject to certain exceptions allowed under applicable law.

- **Deletion.** You have the right to request that we delete the personal information that we maintain about you, subject to certain exceptions. Even after the deletion of your account, some personal information may remain on our servers, such as in technical support logs, server caches, data backups, or email conversations. These will be automatically deleted after a reasonable amount of time, unless we are legally required to retain information for longer, or unless there is a legitimate business reason (e.g. security and fraud prevention or financial record-keeping). We are not required to delete any information which has been aggregated or de-identified in accordance with Section 5.

- **No Discrimination.** You have the right not to be discriminated against for exercising these rights.

- **Appeals.** You have a right to appeal decisions concerning your ability to exercise your consumer rights.

- **Submission of Requests.** You may exercise the above rights by emailing us at privacy@amplify.com. Note that we may deny certain requests, or fulfill a request only in part, based on our legal rights and obligations. For example, we may retain personal information as permitted by law, such as for tax or other record keeping purposes, to maintain an active account, and to process transactions and facilitate customer requests.

- **Authorized Agent.** You may designate an authorized agent to make a request on your behalf. When submitting the request, please ensure the authorized agent identifies himself/herself/itself as an authorized agent and can show written permission from you to represent you. We may contact you directly to confirm that you have authorized the agent to act on your behalf and confirm your identity.

- **Verification.** Whether you submit a request directly on your own behalf, or through an authorized agent, we will take reasonable steps to verify your identity prior to responding to your requests. The verification steps will vary depending on the sensitivity of the personal information and whether you have an account with us.

  Note for students and other Authorized Users who engage with Amplify in connection with a School Customer's use of Amplify: Because Amplify provides the Products to School Customers and Authorized Users as a "School Official," we collect, retain, use, and disclose Student Data only for or on behalf of our School Customers and Authorized Users for educational purposes, including the purpose of providing the Products specified in our Agreement with the School Customer and for no other commercial purpose. Accordingly, we act as a "service provider" for our School Customers under the CCPA.

If you have any questions or would like to exercise your California rights, please contact your school directly.

4. **Notice for European Economic Area and United Kingdom Customers**

If you represent a school in the United Kingdom or European Economic Area, you can review our standard template DPA with attached SCCs here. If the school would like to enter into that DPA (and attached SCCs) with Amplify, please send an email to privacy@amplify.com with the following information about the school: (i) name, (ii) address, (iii) telephone number, (iv) signatory name, (v) signatory title, and (vi) signatory email address, and (vii) teacher.desmos.com account usernames. We will then send the school's signatory a copy of the DPA for electronic signatures and arrange for signature by Amplify's authorized representative.

Amplify collects personal data for the purposes described in Section 3 of this Privacy Policy. We rely on the following lawful bases for our processing activities:

- Consent;
- Pursuant to a contract with the user of our Products;
- To comply with our legal obligations; or
- When we have a legitimate interest in doing so, which is not outweighed by the risks to the individual.