EDUCATION LAW 2-d RIDER

New York State Education Law 2-d was enacted in 2014 to address concerns relative to securing certain personally identifiable information. In order to comply with the requirements of Education Law 2-d, educational agencies and certain third-party contractors who contract with educational agencies must take certain additional steps to secure such data. These steps include enacting and complying with a Parents' "Bill of Rights" relative to protected data, ensuring that each third-party contractor has a detailed data privacy plan in place to ensure the security of such data, and that each third-party contractor sign a copy of the educational agency's Parents' Bill of Rights, thereby signifying that the third-party contractor will comply with such Parents' Bill of Rights. This Agreement is subject to the requirements of Education Law 2-d and CommonLit, Inc. (the "Contractor") is a covered third-party contractor.

In order to comply with the mandates of Education Law 2-d, and notwithstanding any provision of the Agreement between the Shoreham-Wading River Central School District (the "District") and Contractor to the contrary, Contractor agrees as follows:

1. Contractor will treat "Protected Data" (as defined below) as confidential and shall protect the nature of the Protected Data by using the same degree of care, but not less than a reasonable degree of care, as the Contractor uses to protect its own confidential data, so as to prevent the unauthorized dissemination or publication of Protected Data to third-parties. Contractor shall not disclose Protected Data other than to those of its employees or agents who have a need to know such Protected Data under this Agreement. Contractor shall not use Protected Data for any other purposes than those explicitly provided for in this Agreement. All Protected Data shall remain the property of the disclosing party. As more fully discussed below, Contractor shall have in place sufficient internal controls to ensure that the District's Protected Data is safeguarded in accordance with all applicable laws and regulations, including, but not limited to, the Children's Internet Protection Act ("CIPA"), the Children's Online Privacy Protection Act ("COPPA"), the Protection of Pupil Rights Amendment ("PPRA"), the Family Educational Rights and Privacy Act ("FERPA"), and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and Part 121 of the Regulations of the Commissioner of Education, as it may be amended from time-to-time if applicable.

"**Protected Data**" includes any information rendered confidential by New York State ("State") or federal law, including, but not limited to student data, student demographics, scheduling, attendance, grades, health and discipline tracking, and all other data reasonably considered to be sensitive or confidential data by the District. Protected Data also includes any information protected under Education Law 2-d including, but not limited to:

> "Personally identifiable information" from student records of the District as that term is defined in § 99.3 of FERPA,
>
> -AND-
>
> Personally identifiable information from the records of the District relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§3012-c and 3012-d.

2. Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any Protected Data shall comply with New York State Education Law § 2-d. As applicable, Contractor agrees to comply with District policy(ies) on data security and privacy. Contractor shall promptly reimburse the District for the full cost of notifying a parent, eligible student, teacher, or principal of an unauthorized release of Protected Data by Contractor, its subcontractors, and/or assignees. In the event this Agreement expires, is not renewed or is terminated, Contractor shall return all of the District's data unless otherwise provided, including any and all Protected Data, in its possession by secure transmission.

Contractor's Data Security and Privacy Plan Requirements

3. Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any of the District's Protected Data, shall maintain a Data Security and Privacy Plan which includes the following elements:

a. Outline how the Contractor will implement all State, federal, and local data security and privacy requirements over the life of the Agreement, consistent with the District's data security and privacy policy;
b. Specify the administrative, operational and technical safeguards and practices in place to protect personally identifiable information that Contractor will receive under the contract;
c. Demonstrate Contractor's compliance with the requirements of 8 NYCRR Part 121.3(c);
d. Specify how officers or employees of the Contractor and its assignees who have access to student data, or teacher or principal data receive or will receive training on the federal and State laws governing confidentiality of such data prior to receiving access;
e. Specify how Contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;
f. Specify how Contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the District;
g. Describe whether, how and when data will be returned to the District, transitioned to a successor contractor, at the District's option and direction, deleted or destroyed by the Contractor when the Agreement is terminated or expires.

4. Pursuant to the Plan, Contractor will:

a. Have adopted technologies, safeguards and practices that align with the NIST Cybersecurity Framework referred to in Part 121.5;
b. Comply with the data security and privacy policy of the District; Education Law § 2-d; and Part 121;
c. Limit internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services;
d. Have prohibited the use of personally identifiable information for any purpose not explicitly authorized in this contract;
e. Have prohibited the disclosure of personally identifiable information to any other party without the prior written consent of the parent or eligible student:

i. except for authorized representatives of Contractor such as a subcontractor or assignee to the extent they are carrying out the Agreement and in compliance with State and federal law, regulations and its Agreement with District; or
ii. unless required by statute or court order and Contractor has provided a notice of disclosure to the department, District Board of Education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.

f. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in its custody;
g. Use encryption to protect personally identifiable information in its custody while in motion or at rest; and
h. Not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

Contractor understands and agrees that it is responsible for submitting the above-referenced Data Security and Privacy Plan to the District prior to the start of the term of this Agreement. A copy of Contractor's Data Security and Privacy Plan is attached hereto as Exhibit "C". Further, Contractor shall sign a copy of the District's Parents Bill of Rights attached hereto as Exhibit "A".

Contractor's Supplemental Information Requirements

5. Contractor understands that, as part of the District's obligations under New York State Education Law § 2-d, Contractor is responsible for providing the District with supplemental information to be included in the District's Parents' Bill of Rights. Such supplemental information shall include:

a. The exclusive purposes for which the student data or teacher or principal data will be used;
b. How the Contractor will ensure that the subcontractors, persons or entities that the Contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements;
c. When the agreement expires and what happens to the student data or teacher or principal data upon expiration of the Agreement;
d. If and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected; and
e. Where the student data or teacher or principal data will be stored (described in such a manner as to protect data security), and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.

The supplemental information required to be provided is included as Exhibit "B" and is incorporated by reference herein and made a part of this Agreement.

6. In the event of a breach of the within confidentiality and data security and privacy standards provision and unauthorized release of student data or teacher or principal data, Contractor shall promptly and without unreasonable delay notify the District and advise it as to the nature of the breach and steps Contractor has taken to minimize said breach. Said notification must be made in the most expedient way possible and without unreasonable delay but within no more than seven

(7) calendar days of discovery of the breach. Notification required hereunder shall be made in writing and must, to the extent available, include a description of the breach, date of incident, date of discovery, the types of personally identifiable information affected, the number of records affected, a description of Contractor's investigation, and contact information for Contractor's representatives who can assist the District. Notification must be sent to the District's Superintendent of Schools with a copy to the District's Data Protection Officer. Notifications required under this paragraph must be provided to the District. at the following address:

Mr. Gerard Poole
Shoreham-Wading River Central School District
250B Rt. 25A
Shoreham, NY 11786

7. In the event that Contractor fails to notify the District of a breach in accordance with Education Law § 2-d, and/or Part 121 of the Regulations of the Commissioner of Education, said failure shall be punishable by a civil penalty of the greater of five thousand dollars ($5,000) or up to ten dollars ($10) per student, teacher and principal whose data was released, provided that the maximum penalty imposed shall not exceed the maximum penalty imposed under General Business Law § 899-aa(6)(a).

8. Except as provided in Education Law § 2-d(6)(d), in the event Contractor violates Education Law § 2-d, said violation shall be punishable by a civil penalty of up to one thousand dollars ($1,000). A second violation involving the same data shall be punishable by a civil penalty of up to five thousand dollars ($5,000). Any subsequent violation involving the same data shall be punishable by a civil penalty of up to ten thousand dollars ($10,000). Each violation shall be considered a separate violation for purposes of civil penalties and the total penalty shall not exceed the maximum penalty imposed under General Business Law § 899-aa(6)(a).

9. Contractor agrees that it will cooperate with the District and law enforcement, where necessary, in any investigations into a breach. Any costs incidental to the required cooperation or participation of the Contractor or its employees, agents, affiliates, or authorized users, as related to such investigations, will be the sole responsibility of the Contractor if such breach is attributable to the Contractor or its subcontractors.

10. Upon termination of this Agreement, Contractor shall return or, at the District's option, destroy all confidential information obtained in connection with the services provided herein and/or Protected Data. Destruction of the confidential information and/or Protected Data shall be accomplished utilizing an approved method of confidential destruction, including, shredding, burning or certified/witnessed destruction of physical materials and verified erasure of magnetic media using approved methods of electronic file destruction. Contractor further agrees that the terms and conditions set forth herein shall survive the expiration and/or termination of this Agreement.

11. In the event Contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the Contractor by State and federal law and Agreement shall apply to the subcontractor.

12. Where a parent or eligible student requests a service or product from Contractor and provides express consent to the use or disclosure of personally identifiable information by the third-party Contractor for purposes of providing the requested product or service, such use by the third-party Contractor shall not be deemed a marketing or commercial purpose prohibited by the Plan.

Contractor: **CommonLit, Inc.**

Signature: Tony Viviani **Date:** May 2, 2025

Printed Name: **Tony Viviani** **Title:** **Dir Legal & Compliance**

EXHIBIT "A"

Shoreham-Wading River Central School District
Parents' Bill of Rights

Parents and guardians of students attending or seeking to enroll in the Shoreham-Wading River CSD are advised that they have the following rights with regard to student data under New York State Education Law.

1. A student's personally identifiable information will not be released or sold by the District for any commercial purposes.

2. A parent or guardian has the right to inspect and review the complete contents of their child's education record.

3. State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred. Third Party contractors are required to employ technology, safeguards, and practices that align with the National Institute of Standards and Technology Cybersecurity Framework.

4. A complete list of all student data elements collected by New York State is available for public review at https://www.nysed.gov/data-privacy-security/student-data-inventoryor by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, NY 12234.

5. Parents and guardians have the right to have complaints about possible breaches of student data addressed. 89 Washington Avenue Albany, NY 12234

   Complaints should be addressed to:

   Alan Meinster, Assistant Superintendent for Curriculum, Instruction, and Assessment; DPO
   250B Route 25A
   Shoreham, NY 11786
   (631) 821-8100
   Or with NYSED
   Chief Privacy Officer
   New York State Education Department
   Email: Privacy@nysed.gov

6. This Bill of Rights will be included with every contract entered by the District with an outside contractor if the contractor will receive student, teacher, or principal data. This Bill of Rights will be supplemented to include information about each contract that the District enters into with an outside contractor receiving confidential student, teacher, or principal data, including the exclusive purpose (s) for which the data will be used, how the contractor will ensure confidentiality and data protection and security requirements, the date of expiration of the contract and what happens to the data upon the expiration of the contract, if and how the accuracy of the data collected can be challenged, where the data will be stored and the security protections that will be taken.

7. In the event of a data breach or unauthorized disclosure of students' personally identifiable information, third party contractors are required by law to notify the School District within seven (7) days of discovery of the breach or unauthorized disclosure.

8. In the event of a data breach or unauthorized disclosure of students' personally identifiable information, the District will notify the public via written notice, electronic notice through the District's electronic communication platform, or Telephone notification.

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

10. Parents may access the State Education Department's Parent's Bill of Rights at: https://www.nysed.gov/sites/default/files/programs/data-privacy-security/parents-bill-of-rights_2.pdf

Contractor: **CommonLit, Inc.**

Signature: Tony Viviani **Date:** May 2, 2025

Printed Name: **Tony Viviani** **Title:** **Dir. Legal & Compliance**

EXHIBIT "B"

Contractor's Supplemental Information

Name of Contractor	**CommonLit, Inc.**
Description of the purpose(s) for which Contractor will receive/access PII	**Provision and improvement of services provided through www.commonlit.org**
Type of PII that Contractor will receive/access	Check all that apply: ☒ Student PII ☐ APPR Data
Agreement Term	Agreement Start Date: May 2, 2025 Agreement End Date: 30 days following written request for termination of services.
Subcontractor Written Agreement Requirement	Contractor will not utilize subcontractors without a written agreement that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the Contractor by State and federal laws and regulations, and the Agreement. (check applicable option): ☐ Contractor will not utilize subcontractors. ☒ Contractor will utilize subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Contractor shall: • Securely transfer data to District, or a successor contractor at the District's option and written discretion, in a format agreed to by the parties. • Securely delete and destroy data.
Challenges to Data Accuracy	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the District. If a correction to data is deemed necessary, the District will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the District's written request.
Secure Storage and Data Security	Please describe where PII will be stored and the protections taken to ensure PII will be protected (check all that apply): ☒ Using a cloud or infrastructure owned and hosted by a third-party. ☐ Using Contractor owned and hosted solution. ☐ Other: Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data: Data will be encrypted while in motion and at rest.
Encryption	Data will be encrypted while in motion and at rest.

Contractor: **CommonLit, Inc.**

Signature: Tony Viviani **Date:** May 2, 2025

Printed Name: **Tony Viviani** **Title:** **Dir. Legal & Compliance**

EXHIBIT "C"

Contractor's Data Security & Privacy Plan

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN IS ATTACHED HERETO AND INCORPORATED HEREIN.

Privacy Policy

1. What is CommonLit?

CommonLit, Inc. (collectively with any subsidiaries, "CommonLit", “we”, or “us”) is a non-profit organization that delivers high-quality, free instructional materials to support literacy development for students in grades 3-12. To achieve this goal, we must collect certain information from our users, subject to this Privacy Policy and our Terms of Service.

This Privacy Policy describes our practices regarding information we collect through our web sites, including www.CommonLit.org, mobile features, applications and any other interactive features or services owned or controlled by CommonLit that post a link to this Privacy Policy (each, a "Service" and collectively, the "Services"), as well as any information we collect offline and combine in our databases. Certain features discussed in this Privacy Policy may not be offered on each Service at any particular time. Note that we combine the information we collect from you

through all of our websites, mobile applications, and other Services.

Note about Children: As required by applicable law and our Terms of Service, children under the age of 13 in the U.S. (and a higher age if required by the applicable law in another country) may only use our Services with the express prior consent of a parent or legal guardian. **If you are a Teacher or Administrator, you must obtain all necessary parental consents before allowing students to create an account or use the Services.**

2. What is this policy?

WE FULLY DESCRIBE OUR PRIVACY PRACTICES BELOW IN THIS PRIVACY POLICY. THIS SUMMARY PROVIDES AN OVERVIEW OF SOME IMPORTANT INFORMATION REGARDING OUR USE AND SHARING OF YOUR INFORMATION, AND THIRD PARTIES WHO MAY SERVE ADVERTISEMENTS AND WHO MAY SET COOKIES OR WEB BEACONS OR SIMILAR TRACKING TECHNOLOGIES WHEN YOU USE THE SERVICES. PLEASE READ THE ENTIRE PRIVACY POLICY VERY CAREFULLY. BY USING ANY SERVICE, YOU AGREE TO BE BOUND BY THIS PRIVACY POLICY IN ITS ENTIRETY.

Information collection/How we use your information: We primarily use the information we collect when you use the Services in connection with your relationship with CommonLit, your use of the Services, and for sending you information from us. This may include connecting you to other members of the CommonLit community. Please review the **"What information does CommonLit Collect?"** and **"How does CommonLit use the information it collects?"** sections of this Privacy Policy for a full description of the information we collect, including Personal Information (as defined

below), and how we use that information.

Information Sharing: Remember that if you create a Profile (as defined below) or share personal information with other users on the Services, your information may be visible to others. However, student data will only be visible to their teachers, and students cannot share data with other students. Note that we do not share your Personal Information with third parties for their marketing purposes; however, we may share your Personal Information under certain limited circumstances. For more details, please review the section below entitled **"Will CommonLit share any of the information it collects?"**

Third party analytics providers: We work with analytics service providers and other vendors to provide us with information regarding traffic on the Services, including the pages viewed and the actions users take when visiting the Services and to provide us with information regarding the use of the Services.
CommonLit never conducts advertising or marketing activities on the Services or using Personal Information. Please review **"Third Party Analytics Providers"** for additional information.

3. What information does CommonLit collect?

Information Shared With Us

1. Registration and Other Information You Provide

The Services may collect **"Personal Information"** (which is information that can reasonably be used, alone or in combination with other reasonably available information, to identify or contact a

specific individual). Personal Information includes, but is not limited to, student data, metadata, and user content. This may include a name, email address, username, password, or assessment results. Any information combined with Personal Information will be treated as Personal Information.

2. Your Account Page and Community Forums

Your Account Page: Teachers must create an Account that contains the teacher's name, password, email, role, and school. Students or teachers may create student accounts which contain their names, passwords, grade level, and may contain emails. Teachers cannot view students' Account pages; however, teachers are able to view the name, email, and grade level of each of their students. Teachers may be able to view the name and email address of other teachers at their same school, but cannot view another teacher's Account Page.

Community Communications: The Services may provide teachers the opportunity to participate and post content that would be visible to other teachers, through interactive features and through other communication functionality ("Community Communications").
Note that anything you post to a Community Communication may be visible to others.

3. Third Party Services, Social Media Platforms, and Information Third Parties Provide About You

Third parties may provide us with information about you. For example, if you are on a third party web site, and you opt-in to receive information from us, that third party will forward information

about you to us so that we may contact you as requested.

The Services may permit interactions between the Services and a third party web site or service, such as enabling you to "like" a product within our Services or "share" content to other web sites. If you choose to "like" or "share" content or to otherwise post information from or via the Services to a third party web site, feature or application, that information may be publicly displayed, and the third party web site may have access to information about you and your use of our Services. Similarly, if you publicly post information on a third party platform that references CommonLit or one of the Services, your post may be published on our Services in accordance with terms of that third party. These features may collect your IP address or other Device Identifier, which page you are visiting on our web site, and may set a cookie to enable the third party feature to function properly. Third party features and applications are either hosted by a third party or hosted directly on our Services. Your interactions with these features are governed by the privacy policy(ies) of the company(ies) providing it.

The information we collect is subject to this Privacy Policy. The information collected and stored by the third party remains subject to the third party's privacy practices, including whether the third party continues to share information with us, the types of information shared, and your choices with regard to what is visible to others on that third party web site and service. The third party may allow you to remove the application or feature, in which case we will no longer collect information about you through the application or feature, but we may retain the information previously collected in compliance with all applicable laws.

Information We Collect Automatically

Like other web sites and online services, we and our analytics providers, vendors and other third party service providers may automatically collect certain "Usage Information" whenever you access and use the Services. For example, we may collect information regarding when a user downloads resources such as pdfs or the pages a user accesses.

Usage Information may include the browser and operating system you are using, the URL that referred you to our Services (if applicable), the search terms you entered into a search engine that lead you to our Services (if applicable), all of the areas within our Services that you visit (including information about any ads you may view), and the time of day you used the Services, among other information. We may use Usage Information for a variety of purposes, including to select appropriate content to display to you and to enhance or otherwise improve the Services and our products.

In addition, we automatically collect your IP address or other unique identifier ("Device Identifier") for any computer, mobile phone or other device (any, a "Device") you may use to access the Services. A Device Identifier is a number that is automatically assigned to your Device used to access a Service, and our servers identify your Device by its Device Identifier. Some mobile service providers may also provide us or our third party service providers with information regarding the physical location of the Device used to access a Service, internet service provider (ISP), date and time of your visit, browser language, browser type,

referring and exit pages and URLs, amount of time spent on particular pages, which parts of our Services you use, which links you click, search terms, operating system, traffic and related statistics, keywords, and/or other general browsing or usage data. Usage Information is generally non-identifying, but if we associate it with you as a specific and identifiable person, we treat it as Personal Information.

Usage Information is collected via tracking technologies, including:

1. Cookies: Our Services utilize Cookies to improve your current and future experience by allowing us to understand your usage of our Services. For example, cookies help our systems recognize you if you return to our Services shortly after exiting them. Cookies are small text files stored on your computer that allow us to personalize the content of our Services. Cookies can be turned off via your browser settings if you so choose. However, if you turn your cookies off, some features of our Services may not function properly.

2. An Embedded Script: is programming code that is designed to collect information about your interactions with the Services, such as the links you click on. The code is temporarily downloaded onto your computer or other device from our server or a third party service provider and is deactivated or deleted when you disconnect from the Services.

In addition, we may use a variety of other technologies that collect similar information for security and fraud detection purposes.

3. HTML5: We use Local Storage Objects (LSOs) such as HTML5 to store content, information and

preferences. Third parties with whom we partner to provide certain features on our site use LSOs such as HTML 5 & Flash to collect and store information.

Various browsers may offer their own management tools for removing HTML5 LSOs.

How We Respond To Do Not Track Signals:

Please note that your browser setting may allow you to automatically transmit a "Do Not Track" (DNT) signal to websites and online service you visit. DNT is a privacy preference that users can set in certain web browsers to inform websites and services that they do not want certain information about their webpage visits collected over time and across websites or online services. However, we do not recognize or respond to browser-initiated DNT signals, as the internet industry is still working to determine what DNT means, how to comply with DNT, and how to create a common approach to responding to DNT. To find out more about "Do Not Track", please visit http://www.allaboutdnt.com.

4. How does CommonLit use the information it collects?

We may use information about you, including Personal Information, the information you provide in your Profile, User Content, and Usage Information to:

1. Allow you to participate in features we offer or to provide related customer service, including, without limitation, to respond to your questions, complaints or comments;
2. Tailor content, recommendations and offers we display to you, both on the Services and elsewhere

online;
4. Process your registration with our Services, including verifying your e-mail address is active and valid;
5. Improve the Services and for internal business purposes, including the measurement of ad effectiveness;
6. Contact you with regard to your use of the Services and, in our discretion, changes to our policies; and
7. Permit other CommonLit users to contact you, and vice versa; and
8. As described in the Privacy Policy and for purposes disclosed at the time you provide your information or otherwise with your consent.

Please note that information submitted on the Services via a "Contact Us" or other similar function may not receive a response. We will not use the information provided via these functions to contact you for marketing purposes unrelated to your request unless you agree otherwise.

5. Will CommonLit share any of the information it collects?

CommonLit does not share your Personal Information with third parties for their marketing purposes in compliance with all applicable laws (including California Business & Professions Code section 22584 ("SOPIPA"), and California Education Code section 49073.1). CommonLit may share non-Personal Information, such as aggregate or de-identified user statistics, demographic information and Usage Information with third parties.

We also may share your Personal Information with third parties with your consent (if permissible under applicable law), as disclosed at the time you provide us with information, and as described below or otherwise in this Privacy Policy:

1. Service Providers

We will share your Personal Information with third parties to provide services to us or you in connection with the Services, but subject to confidentiality obligations which limit their use and disclosure of such information. For example, we may provide your Personal Information to companies that provide services to help us with our business activities, sending our emails, or offering customer service. If you purchase any merchandise, our billing partner will receive billing, shipping and financial information (e.g., credit card numbers) necessary to process your charges, including your postal and e-mail addresses, depending on your payment method.

2. Administrative, Legal Reasons & Academic Integrity Investigations

We may also disclose your information, including Personal Information, in response to a subpoena, court order, or when otherwise required by law; in response to bankruptcy proceedings; to defend our rights; in response to a request from law enforcement; to provide information to a claimed owner of intellectual property who claims that content you have provided to us infringes on their rights; upon request of or as otherwise authorized by an academic institution connected to an investigation into academic integrity; to protect and/or defend any applicable Terms of Use or other policies applicable to the Services; or to

protect the personal safety, rights, property or security of any organization or individual.

We may also use Device Identifiers, including IP addresses, to identify users, and may do so in cooperation with copyright owners, Internet service providers, wireless service providers or law enforcement agencies in our discretion. These disclosures may be carried out without your consent or without notice to you.

3. Business Transitions

CommonLit may share Personal Information with its parent, subsidiaries and affiliates, and investors primarily for business and operational purposes so long as any recipient agrees to comply with this Privacy Policy and applicable law with regard to such Personal Information. In the event that CommonLit goes through a business transition, such as a merger, acquisition by another company, or sale of all or a portion of its assets, bankruptcy, or other corporate change, including, without limitation, during the course of any due diligence process, your information, including Personal Information, will likely be among the assets transferred.
You will be notified via email and/or a prominent notice on Services of any completed change in ownership or uses of your Personal Information, as well as any choices you may have regarding your Personal Information. This Privacy Policy will become binding upon the new owner of the information until amended.

4. Testimonials

We display personal testimonials of satisfied adult users on our Services in addition to other endorsements. With your consent, we may post

your testimonial along with your name. If you wish to update or delete your testimonial, you can contact us via email by clicking here.

6. How does CommonLit work with third parties?

No Third Party Advertising

CommonLit will never use any Student Data to advertise or market to students or their parents. We will not mine Student Data for any purposes other than those agreed to by the parties. Data mining or scanning of user content for the purpose of advertising or marketing to students or their parents is prohibited.

Third Party Analytics Providers

We work with analytics service providers and other vendors to provide us with information regarding traffic on the Services, including the pages viewed and the actions users take when visiting the Services and to provide us with information regarding the use of the Services.

Third Party Content, Links to Other Sites, and CommonLit Content Found Outside of the Services

Certain content provided through the Services may be hosted and served by third parties. In addition, the Services may link to third party web sites or content over which CommonLit has no control and which are governed by the privacy policies and business practices of those third

parties. In addition, third-parties may have different privacy policies which apply to such third party use of your information.

Please also note that CommonLit content may be included on web pages and web sites that are not associated with us and over which we have no control. These third parties may independently collect data. CommonLit is not responsible or liable for the privacy practices or business practices of any third party.

7. What happens if I access CommonLit's services through a mobile device?

If you use the Services through a mobile device or one of our mobile applications, you agree that CommonLit may store and use that information for security purposes (for example, for user verification or authentication and to ensure that our APIs are being used appropriately).

8. How does CommonLit protect children's information?

Protecting the privacy of young children is especially important to CommonLit. For that reason, we created certain features designed to help protect Personal Information relating to children who are less than 13 years of age, or higher age if required by applicable law ("Child Users").

CommonLit does not knowingly permit Child Users to use our Services without prior, express consent from a parent or legal guardian, except through agreements with schools or districts or as otherwise permitted under the Children's Online Privacy Protection Rule (COPPA) and the Family Educational Rights and Privacy Act (FERPA). If we learn that Personal Information of a Child User has been collected on our Services without prior parental consent, then we will take appropriate steps to delete this information. If you are a parent or guardian ("Parent") and discover that your child under the age of 13 (or a higher age if required by applicable law) has a registered account with our Services without your consent, please contact your child's school and alert CommonLit at security@commonlit.org and request that we delete that child's personal information from our systems.

How does a child register and use the services?

Child Users cannot obtain a User Account without first receiving a prompt from their school. CommonLit obligates schools and teachers (or other authorized individuals) to first obtain any necessary parental consents before permitting children to register for a User Account or use the Services.

What children's information is visible to others?

No student's profile is made available or visible to the public through CommonLit. If a teacher utilizes certain features on a device in the classroom, other students may be able to view information that is displayed by the teacher in the classroom, but

students can't view each other's individual student profiles.

Parents: To review your child's User data you must request the information from your child's teacher.

9. How does CommonLit protect and store my information?

CommonLit takes data security very seriously. CommonLit takes commercially reasonable technical, physical, and administrative security measures designed to protect the Personal Information submitted to us, both during transmission and once we receive it. Such measures vary depending on the sensitivity of the information at issue. Measures taken to protect your data include:

- We continually test CommonLit's security practices for vulnerabilities
- We periodically review our information collection, storage and processing practices, including physical security measures, to guard against unauthorized access to systems
- We continually develop and implement features to keep your personal information safe - for example, all traffic to and from our application is over secure, encrypted protocols (SSL/TLS).
- We ensure passwords are stored securely using encryption and salted one-way hashing
- We also operate a 'bug bounty' security program to encourage an active community of third party security researchers to report any security bugs to us. More information on this is available by contacting us at security@commonlit.org.
- Every CommonLit employee participates in training on the importance of and methods for protecting Personal Information. Training consists of how to remain compliant with federal and state regulations (e.g . FERPA, COPPA, and SOPIPA), CommonLit policies, and general security posturing to protect

student data (including techniques such as Two Factor Authentication, Drive Encryption, creating and managing strong passwords, etc).
- All CommonLit employees are trained in security practices and procedures designed to keep Your Data under strict internal controls.
- Developers peer-review code to make sure changes adhere to best practices for security.
- Administrators are knowledgeable of security practices and harden the infrastructure with necessary patches, monitor security resources for advisories and vulnerabilities, and scan the environment and application to ensure that student information remains secure.

Please note that no method of transmission over the Internet, or method of electronic storage, is 100% secure. Therefore, while we strive to use commercially reasonable means to protect your Personal Information, we cannot guarantee its absolute security.

How will CommonLit handle a data breach or security incident?

In the event that CommonLit becomes aware of a data breach impacting your Personal Information, we will provide notification in compliance with all applicable laws. For example, we may post a notice on our homepage (www.CommonLit.org) or elsewhere on the Service, and may send email to you at the email address you have provided to us. Depending on where you live, you may have a legal right to receive notice of a security breach in writing.
CommonLit has procedures in place that are designed to stop threats that may expose personally identifiable information, restore Services to full functionality, and document and take proactive steps to ensure the incident cannot be repeated. CommonLit will also preserve necessary evidence for investigation by security professionals and law enforcement as appropriate.

In the unlikely event of an unauthorized disclosure of records, CommonLit will follow its internal procedures, which articulates how to report the problem to internal and external stakeholders. The notification process includes any information that can identify which customers and students may have been impacted, the data that may have been accessed, CommonLit's process to inform affected customers, and steps to prevent the incident from happening again as appropriate.

In the unlikely event of an unauthorized disclosure of Data, CommonLit has implemented a process for responding to incidents and notifying affected individuals and, if applicable, law enforcement personnel.

If you have any questions about security on our Services, you can email us by clicking here.

10. How can I opt-out of sharing, providing, or receiving certain information?

Providing Personal Information: You can always decline to share personal information with us, or even block all cookies. However, it's important to remember that many of CommonLit's features may not be accessible, or may not function properly - for example, we may not be able to remember your language preferences for you.
Email Communication: You can opt-out of receiving further communications by clicking the unsubscribe button at the bottom of an email.

11. How can I access and manage my personal information?

You may be able to review the information you provided to us on a Service and make any desired changes to the information, or to the settings for your account on that Service, by logging in to your account for that Service and editing or deleting the information.

12. What communications will I receive from CommonLit and how do I limit them?

CommonLit may send you information by email or may post notices on the CommonLit homepage (www.commonlit.org).

You may choose to stop receiving certain emails from CommonLit by using the unsubscribe button at the bottom of the CommonLit email. However, we reserve the right to send you information on our behalf and on behalf of third parties in connection with providing the Services. If you no longer want to receive information from us, you will need to close your account for that Service.

13. How do I close my account?

If you wish to close your account with one of our Services, please send your request via email by

clicking here and we will remove your Personal Information and Profile, if applicable, from the active databases for the Service(s) you request. Please let us know which Service(s) you wish to close and, if applicable, send your request using an email account that you have registered with CommonLit under your name. You typically will receive a response to a request sent to this account within five business days of our receiving it. Requests to change your email preferences or unsubscribe from all emails may not be made through this email address, but rather must be submitted through one of the channels set out in the previous section.

14. How long does CommonLit keep my information?

Upon termination of your Account, CommonLit will take commercially reasonable steps to delete any Sensitive Information from its live databases in a reasonable amount of time not to exceed ninety (90) days. You understand and agree that CommonLit may continue to have Sensitive Information in archive files or similar databases. You further agree that CommonLit has no obligation to delete aggregated or de-identified information. CommonLit may retain and use aggregated and de-identified information for any purpose that is consistent with laws and regulations.

Even if your account is closed, information may remain in backup or archive records and we may retain certain data relevant to preventing fraud or future abuse or for legitimate business purposes, such as analysis of aggregated, non-personally-

identifiable or de-identified data, account recovery or if required by law. All retained data will continue to be subject to the applicable privacy policy for the Service. Also, if you have posted content on or through the Services, such as in Community Communications, we may not be able to delete it.

15. How will CommonLit notify me of changes to this policy?

We will notify you of material changes to the Privacy Policy on our Website and/or by email, and make additional efforts to notify customers of material changes that impact the treatment of data collected through our Services.

CommonLit may update this Privacy Policy at any time and any changes will be effective upon posting. Upon any update the "Last Updated" date at the top of this policy will be updated. In the event that there are material changes to the way we treat your Personal Information, you are responsible for regularly reviewing this Privacy Policy and your CommonLit account for notice of such modifications. Your continued use of the Services following an update to this Privacy Policy will constitute your acceptance of the updated Privacy Policy.

Our Privacy Policy was last updated on **May 25, 2018**.

16. What if I don't live in the U.S.?

Consent to Transfer

The Services are operated in the United States. If you are located outside of the United States, please be aware that information we collect will be transferred to and processed in the United States. By using the Services, or providing us with any information, you fully understand and unambiguously consent to this transfer, processing and storage of your information in the United States, a jurisdiction in which the privacy laws may not be as comprehensive as those in the country where you reside and/or are a citizen.

Important Information for Users in the European Economic Area

The following information only applies to users in the European Economic Area (EEA), provided that we are the controller of their personal information as described below.

Controller

If you use the Services through your employer, school or another organization, that organization is the controller of your personal information and all questions or requests regarding your rights under European data protection legislation (including the rights described under Your rights below) or the processing of your personal information, should be directed to the organization. CommonLit is the organization's processor and uses your personal information only as instructed by the organization. If you do not use the Services through an organization, CommonLit is the controller of your personal information and can be reached using the contact details in "How can I contact CommonLit with questions" section.

References to “personal information” in this policy are equivalent to “personal data” governed by European data protection legislation.

Legal bases for processing

We process your personal information on the following legal bases:

Processing purpose *(including sharing for such purposes as described above):*
To provide the Services
To communicate with you about the Services
To send you marketing communications
For research and development
To create aggregated or anonymous data for analytics
For security, compliance, fraud prevention and safety
Business transfers
To comply with the law
With your consent

Legal basis: Processing is necessary to provide the Services or to take steps that you request prior to requesting the Services. These processing activities constitute our legitimate interests. We do not use your personal information for activities where your data protection interests override these legitimate interests (unless we have your consent or are otherwise required or permitted to by law). Processing is necessary to comply with our legal obligations. Processing is based on your consent. Where we rely on your consent you have the right to withdraw it anytime in the manner indicated at the time consent is requested.

Please note that we rely on legitimate interests as the basis for processing your data in the limited

circumstances set out below:

- In situations where we obtain your personal data from a source other than you, we process your data on the basis of legitimate interests, until the earlier of either (a) the point at which you provide your consent; or (b) the point at which you ask us to stop processing your data on the basis of our legitimate interests;
- We will archive information about your use of our services, even after you withdraw your consent to our processing of your data. This information will only be used in very limited circumstances, such as for defending legal claims relating to contracts we have with you or a third party and retention for audit purposes relating to commercial contracts; and
- We will use information relating to your use of our services for statistical analysis and research purposes; however, we remove personally-identifying information such as name and email address before we do so.

Cross-border data transfer

In the event that we transfer your personal information out of the EEA to countries not deemed by the European Commission to provide an adequate level of protection for personal information, the transfer will be based on safeguards recognized by the European Commission as providing adequate protection, where required by EU data protection legislation. Please contact us to request further information on the specific mechanism used by us when transferring your personal information out of the EEA.

Your rights

You may ask us to take the following actions in relation to your personal information that we hold:
Access. Provide you with information about our processing of your personal information and give

you access to your personal information.
Correct. Update or correct inaccuracies in your personal information.
Delete. Delete your personal information.
Transfer. Transfer a machine-readable copy of your personal information to you or a third party of your choice.
Restrict. Restrict the processing of your personal information.
Object. Object to our reliance on our legitimate interests as the legal basis of our processing your personal information, where that processing adversely impacts your legal rights.
You may send us these requests by emailing us at help@commonlit.org. We may request information from you to help us confirm your identity and process your request. Applicable law may require or permit us to reject part or all of your request. If we reject your request, we will tell you why, subject to legal restrictions. If you would like to submit a complaint about our use of your personal information or response to your requests regarding your personal information, you may contact us at help@commonlit.org or submit a complaint to the data protection regulator in your jurisdiction. You can find your data protection regulator here.

Retention

We will only retain your personal information for as long as necessary to fulfill the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. To determine the appropriate retention period for personal information, we consider the amount, nature, and sensitivity of the personal information, the potential risk of harm from unauthorized use or disclosure of your personal information, the purposes for which we

process your personal information and whether we can achieve those purposes through other means, and the applicable legal requirements.

18. How can I contact CommonLit with questions?

If you have questions or comments about this Privacy Policy, please contact us via email by clicking here or contact us at: security@commonlit.org.

Last Modified: May 25, 2018