CommonLit

Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

CONTRACT ADDENDUM

Protection of Student Personally Identifiable Information

1. Applicability of This Addendum

The Wayne-Finger Lakes BOCES/EduTech) and CommonLit, Inc. **("Vendor")** are parties to a contract dated May 2, 2024 ("the underlying contract") governing the terms under which BOCES accesses, and Vendor provides, www.commonlit.org ("Product"). Wayne-Finger Lakes BOCES/EduTech use of the Product results in Vendor receiving student personally identifiable information as defined in New York Education Law Section 2-d and this Addendum. The terms of this Addendum shall amend and modify the underlying contract and shall have precedence over terms set forth in the underlying contract and any online Terms of Use or Service published by Vendor.

2. Definitions

2.1. "Protected Information", as applied to student data, means "personally identifiable information" as defined in 34 CFR Section 99.3 implementing the Family Educational Rights and Privacy Act (FERPA) where that information is received by Vendor from BOCES or is created by the Vendor's product or service in the course of being used by BOCES.

2.2. "Vendor" means _____.

2.3. "Educational Agency" means a school BOCES, board of cooperative educational services, school, or the New York State Education Department; and for purposes of this Contract specifically includes Wayne-Finger Lakes BOCES/EduTech.

2.4. "BOCES" means the Wayne-Finger Lakes BOCES/EduTech.

2.5. "Parent" means a parent, legal guardian, or person in parental relation to a Student.

2.6. "Student" means any person attending or seeking to enroll in an educational agency.

2.7. "Eligible Student" means a student eighteen years or older.

2.8. "Assignee" and "Subcontractor" shall each mean any person or entity that receives, stores, or processes Protected Information covered by this Contract from Vendor for the purpose of enabling or assisting Vendor to deliver the product or services covered by this Contract.

2.9. "This Contract" means the underlying contract as modified by this Addendum.

3. Vendor Status

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

4. Confidentiality of Protected Information

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

5. Vendor EmployeeTraining

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

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

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

7. Ownership and Location of Protected Information

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

7.2. BOCESshall have access to the BOCES's Protected Information at all times through the term of this Contract. BOCES shall have the right to import or export Protected Information in piecemeal or in its entirety at their discretion, without interference from Vendor.

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

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

8. Purpose for Sharing Protected Information

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

9. Downstream Protections

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

10. Protected Information and Contract Termination

10.1. The expiration date of this Contract is defined by the underlying contract.

10.2. Upon expiration of this Contract without a successor agreement in place, Vendor shall assist BOCES in exporting all Protected Information previously received from, or then owned by, BOCES.

10.3. Vendor shall thereafter securely delete and overwrite any and all Protected Information remaining in the possession of Vendor or its assignees or subcontractors (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies of shared data) as well as any and all Protected Information maintained on behalf of Vendor in secure data center facilities.

10.4. Vendor shall ensure that no copy, summary or extract of the Protected Information or any related work papers are retained on any storage medium whatsoever by Vendor, its subcontractors or assignees, or the aforementioned secure data center facilities.

10.5. To the extent that Vendor and/or its subcontractors or assignees may continue to be in possession of any de-identified data (data that has had all direct and indirect identifiers removed) derived from Protected Information, they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party.

10.6. Upon request, Vendor and/or its subcontractors or assignees will provide a certification to BOCES from an appropriate officer that the requirements of this paragraph have been satisfied in full.

11. Data Subject Request to Amend Protected Information

11.1. In the event that a parent, student, or eligible student wishes to challenge the accuracy of Protected Information that qualifies as student data for purposes of Education Law Section 2-d, that challenge shall be processed through the procedures provided by the BOCES for amendment of education records under the Family Educational Rights and Privacy Act (FERPA).

11.2. Vendor will cooperate with BOCES in retrieving and revising Protected Information, but shall not be responsible for responding directly to the data subject.

12. Vendor Data Security and Privacy Plan

12.1. Vendor agrees that for the life of this Contract the Vendor will maintain the administrative, technical, and physical safeguards described in the Data Security and Privacy Plan set forth in Attachment C to this Contract and made a part of this Contract.

12.2. Vendor warrants that the conditions, measures, and practices described in the Vendor's Data Security and Privacy Plan:

12.3. align with the NIST Cybersecurity Framework 1.0;

12.4. equal industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection;

12.5. outline how the Vendor will implement all state, federal, and local data security and privacy contract requirements over the life of the contract, consistent with the BOCES data security and privacy policy (Attachment B);

12.6. specify the administrative, operational and technical safeguards and practices it has in place to protect Protected Information that it will receive under this Contract;

12.7. demonstrate that it complies with the requirements of Section 121.3(c) of this Part;

12.8. specify how officers or employees of the Vendor and its assignees who have access to Protected Information receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;

12.9. specify if the Vendor will utilize sub-contractors and how it will manage those relationships and contracts to ensure Protected Information is protected;

12.10. specify how the Vendor will manage data security and privacy incidents that implicate Protected Information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify BOCES; and

12.11. describe whether, how and when data will be returned to BOCES, transitioned to a successor contractor, at BOCES's option and direction, deleted or destroyed by the Vendor when the contract is terminated orexpires.

13. Additional VendorResponsibilities

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

13.1 Vendor shall limit internal access to Protected Information to those individuals and Assignees or subcontractors that need access to provide the contracted services;

13.2 Vendor will not use Protected Information for any purpose other than those explicitly authorized in this Contract;

13.3 Vendor will not disclose any Protected Information to any party who is not an authorized representative of the Vendor using the information to carry out Vendor's obligations under this Contract or to the BOCES unless (1) Vendor has the prior written consent of the parent or eligible student to disclose the information to that party, or (ii) the disclosure is required by statute or court order, and notice of the disclosure is provided to BOCES no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order;

13.4 Vendor will maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Protected Information in its custody;

13.5 Vendor will use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the secretary of the U S. Department of HHS in guidance issued under P.L. 111-5, Section 13402(H)(2);

13.6 Vendor will notify the BOCES of any breach of security resulting in an unauthorized release of student data by the Vendor or its Assignees in violation of state or federal law, or of contractual obligations relating to data privacy and security in the most expedient way possible and without unreasonable delay but no more than seven calendar days after the discovery of the breach; and

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

Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

Signatures

For Wayne-Finger Lakes BOCES/EduTech	For (Vendor Name)
[signature]	Tony Viviani
Date 5/6/24	**Date** May 2, 2024

Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

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

Wayne-Finger Lakes BOCES (EduTech)

Parents' Bill of Rights for Data Privacy and Security

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

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

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

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

Revised October 2019

Signatures

For Wayne-Finger Lakes BOCES/EduTech	**For (Vendor Name)**
	Tony Viviani
Date	**Date**
5/6/24	May 2, 2024

Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

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

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

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

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

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

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

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

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

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

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

b) Personally Identifiable Information, as applied to student data, means 40 personally identifiable information as defined in section 99.3 of Title 34 of the Code of 41 Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 42 U.S.C 1232-g, and as applied to teacher and principal data, means personally 43 identifying information as such term is defined in Education Law §3012-c(10).

c) Breach means the unauthorized access, use, or disclosure of student data 9 and/or teacher or principal data. Good faith acquisition of personal information by an employee or agent of the BOCES for the purposes of the BOCES is not a breach of the security of the system, provided that private information is not used or subject to unauthorized disclosure.

Notification Requirements
Methods of Notification

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

a) Written notice;

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

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

In the event that any residents are to be notified, the BOCES shall notify the New York State Chief Privacy Officer, the New York State Cyber Incident Response Team, the office of Homeland Security, and New York State Chief Security Officer as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected residents.
The Superintendent or his/her designee will establish and communicate procedures for parents, eligible students, and employees to file complaints about breaches or unauthorized releases of student, teacher or principal data (as set forth in 8 NYCRR §121.4). The Superintendent is also authorized to promulgate any and all other regulations necessary and proper to implement this policy.

Data Protection Officer

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

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

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

Annual Data Privacy and Security Training

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

References:

Education Law §2-d

8 NYCRR §121

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

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

Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

Attachment C – Vendor's Data Security and Privacy Plan

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

(Vendor can attach)

Addendum B

PARENTS' BILL OF RIGHTS – SUPPLEMENTAL INFORMATION ADDENDUM

1. **EXCLUSIVE PURPOSES FOR DATA USE**: The exclusive purposes for which "student data" or "teacher or principal data" (as those terms are defined in Education Law Section 2-d and collectively referred to as the "Confidential Data") will be used by CommonLit, Inc. (the "Contractor") are limited to the purposes authorized in the contract between the Contractor and the Wayne-Finger Lakes BOCES/EduTech (the "BOCES") dated May 2, 2024(the "Contract").

2. **SUBCONTRACTOR OVERSIGHT DETAILS**: The Contractor will ensure that any subcontractors, or other authorized persons or entities to whom the Contractor will disclose the Confidential Data, if any, are contractually required to abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable State and Federal laws and regulations (e.g., the Family Educational Rights and Privacy Act ("FERPA"); Education Law §2-d; 8 NYCRR Part 121).

3. **CONTRACT PRACTICES**: The Contract commences and expires on the dates set forth in the Contract, unless earlier terminated or renewed pursuant to the terms of the Contract. On or before the date the Contract expires, protected data will be exported to the BOCES in **an agreed upon (insert data format)** format and/or destroyed by the Contractor as directed by the BOCES.

4. **DATA ACCURACY/CORRECTION PRACTICES**: A parent or eligible student can challenge the accuracy of any "education record", as that term is defined in FERPA, stored by the BOCES in a Contractor's product and/or service by following the BOCES' procedure for requesting the amendment of education records under FERPA. Teachers and principals may be able to challenge the accuracy of APPR data stored by the BOCES in Contractor's product and/or service by following the appeal procedure in the BOCES' APPR Plan. Unless otherwise required above or by other applicable law, challenges to the accuracy of the Confidential Data shall not be permitted.

5. **SECURITY PRACTICES**: Confidential Data provided to Contractor by the BOCES will be stored using a third party cloud storage provider, AWS, in the continental United States (**insert location**). The measures that Contractor takes to protect Confidential Data will align with the NIST Cybersecurity Framework including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.

6. **ENCRYPTION PRACTICES**: The Contractor will apply encryption to the Confidential Data while in motion and at rest at least to the extent required by Education Law Section 2-d and other applicable law.

Signature: Tony Viviani

Date: May 2, 2024

Privacy Policy

Last Modified: May 25, 2018

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 publically 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)*	**Legal basis**
To provide the Services	Processing is necessary to provide the Services or to take steps that you request prior to requesting the Services.
To communicate with you about the ServicesTo send you marketing communicationsFor research and developmentTo create aggregated or anonymous data for analytics For security, compliance, fraud prevention and safetyBusiness transfers	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).
To comply with law	Processing is necessary to comply with our legal obligations.
With your consent	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.