

CALIFORNIA STUDENT DATA PRIVACY AGREEMENT

IRVINE UNIFIED SCHOOL DISTRICT

and

OXFORD UNIVERSITY PRESS

October 17, 2018

This California Student Data Privacy Agreement ("DPA") is entered into by and between the IRVINE UNIFIED SCHOOL DISTRICT (hereinafter referred to as "LEA") and OXFORD UNIVERSITY PRESS (hereinafter referred to as "Provider") on October 17, 2018. The Parties agree to the terms as stated herein.

RECITALS

WHEREAS, the Provider has agreed to provide the Local Education Agency ("LEA") with certain digital educational services ("Services") pursuant to various Purchase Orders ("Service Agreement"); and

WHEREAS, in order to provide the Services described in the Service Agreement, the Provider may receive and the LEA may provide documents or data that are covered by several Federal and State statutes, among them, the Federal Educational and Privacy rights Act ("FERPA") at 20 U.S.C. 1232g, Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. 6501-6502; Protection of Pupil Rights Amendment ("PPRA") 20 U.S.C. 1232 h; and

WHEREAS, the documents and data transferred from California LEAs are also subject to several California student privacy laws, including AB 1584, found at California Education Code Section 49073 .1 and the Student Online Personal Information Protection Act (sometimes referred to as either "SB 1177" or "SOPIPA") found at California Business and Professions Code section 22584; and

WHEREAS, the Parties wish to enter into this DPA to ensure that the Service Agreement conforms to the requirements of the privacy laws referred to above and to establish implementing procedures and duties; and

WHEREAS, the Provider may, by signing the "General Offer of Privacy Terms", agree to allow other LEAs in California the opportunity to accept and enjoy the benefits of this DPA for the Services _____ described herein, without the need to negotiate terms in a separate DPA.

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA.** The purpose of this DPA is to describe the duties and responsibilities to protect student data transmitted to Provider from the LEA pursuant to the Service Agreement, including compliance with all applicable privacy statutes, including the FERPA, PPRA, COPPA, SB 1177 (SOPIPA), and AB 1584. In performing these services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA. Control duties are set forth below.
2. **Nature of Services Provided.** The Provider has agreed to provide the following digital educational services described below and as may be further outlined in Exhibit "A" hereto:

Access to Oxford English Dictionary online.

3. **Student Data to Be Provided.** In order to perform the Services described in the Service Agreement, LEA shall provide the categories of data described below or as indicated in the Schedule of Data, attached hereto as Exhibit "B":

4. **DPA Definitions.** The definition of terms used in this DPA is found in Exhibit "C". In the event of a conflict, definitions used in this DPA shall prevail over term used in the Service Agreement.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA.** All Student Data or any other Pupil Records transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data or any other Pupil Records contemplated per the Service Agreement shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEAs as it pertains to the use of student data notwithstanding the above. Provider may transfer pupil-generated content to a separate account, according to the procedures set forth below.
2. **Parent Access.** Provider and the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review personally identifiable information on the pupil's records, correct erroneous information, and procedures for the transfer of pupil-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner to the LEA's request for personally identifiable information in a pupil's records held by the Provider to view or correct as necessary. In the event that a parent of a pupil or other individual contacts the Provider to review any of the Pupil Records of Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.
3. **Separate Account.** Provider shall, at the request of the LEA, transfer Student generated content to a separate student account.
4. **Third Party Request.** Should a Third Party, including law enforcement and government entities, contact Provider with a request for data held by the Provider pursuant to the Services, the Provider shall redirect the Third Party to request the data directly from the LEA. Provider shall notify the LEA in advance of a compelled disclosure to a Third Party unless legally prohibited.

5. **No Unauthorized Use.** Provider shall not use Student Data or information in a Pupil Record for any purpose other than as explicitly specified in the Service Agreement.
6. **Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions pursuant to the Service Agreement, whereby the Subprocessors agree to comply with all applicable data protection laws.

ARTICLE III: DUTIES OF LEA

1. **Provide Data In Compliance With FERPA.** LEA shall provide data for the purposes of the Service Agreement in compliance with the Family Educational Rights and Privacy Act ("FERPA"), 20 U.S.C. section 1232 g, AB 1584 and the other privacy statutes quoted in this DPA.
2. **Reasonable Precautions.** LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted data.
3. **Unauthorized Access Notification.** LEA shall notify Provider promptly of any known or suspected unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.
4. **District Representative.** At request of Provider, LEA shall designate an employee or agent of the District as the District representative for the coordination and fulfillment of the duties of this DPA.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance.** The Provider shall comply with all California and Federal laws and regulations pertaining to data privacy and security, including but not limited to FERPA, COPPA, PPRA, AB 1584, and SOPIPA.
2. **Authorized Use.** The data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services stated in the Service Agreement and/or otherwise authorized under the statutes referred to in subsection (1), above.
3. **Employee Obligation.** Provider shall require all employees and agents who have access to Student Data to comply with all applicable provisions of FERPA laws with respect to the data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.

4. **No Disclosure.** Provider shall not disclose any data obtained under the Service Agreement in a manner that could identify an individual student to any other entity in published results of studies as authorized by the Service Agreement. Deidentified information may be used by the vendor for the purposes of development and improvement of educational sites, services, or applications.
5. **Disposition of Data.** Provider shall dispose of all personally identifiable data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained and transfer said data to LEA or LEA's designee within 60 days of the date of termination and according to a schedule and procedure as the Parties may reasonably agree. Nothing in the Service Agreement authorizes Provider to maintain personally identifiable data obtained under the Service Agreement beyond the time period reasonably needed to complete the disposition. Disposition shall include (1) the shredding of any hard copies of any Pupil Records; (2) Erasing; or (3) Otherwise modifying the personal information in those records to make it unreadable or indecipherable. Provider shall provide written notification to LEA when the Data has been disposed. The duty to dispose of Student Data shall not extend to data that has been de-identified or placed in a separate Student account, pursuant to the other terms of the DPA. Nothing in the Service Agreement authorizes Provider to maintain personally identifiable data beyond the time period reasonably needed to complete the disposition.
6. **Advertising Prohibition.** Provider is prohibited from using Student Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing, advertising, or other commercial efforts by a Provider; or (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Service to Client.

ARTICLE V: DATA PROVISIONS

1. **Data Security.** The Provider agrees to abide by and maintain adequate data security measures to protect Student Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of Provider are set forth below. Provider may further detail its security programs and measures in in Exhibit "D" hereto. These measures shall include, but are not limited to:
 - a. **Passwords and Employee Access.** Provider shall make best efforts practices to secure usernames, passwords, and any other means of gaining access to the Services or to Student Data, at a level suggested by Article 4.3 of NIST 800-63-3. Provider shall only provide access to Student Data to employees or contractors that are performing the Services. As stated elsewhere in this DPA, employees with access to Student Data shall have signed confidentiality agreements regarding said Student Data. All employees with access to Student Records shall pass criminal background checks.
 - b. **Destruction of Data.** Provider shall destroy all personally identifiable data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained or transfer said data to LEA or LEA's designee, according to a schedule and procedure as the parties may reasonable agree. Nothing in the Service Agreement

authorizes Provider to maintain personally identifiable data beyond the time period reasonably needed to complete the disposition.

- c. **Security Protocols.** Both parties agree to maintain security protocols that meet industry best practices in the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. Provider shall maintain all data obtained or generated pursuant to the Service Agreement in a secure computer environment and not copy, reproduce, or transmit data obtained pursuant to the Service Agreement, except as necessary to fulfill the purpose of data requests by LEA.
- d. **Employee Training.** The Provider shall provide periodic security training to those of its employees who operate or have access to the system. Further, Provider shall provide LEA with contact information of an employee who LEA may contact if there are any security concerns or questions.
- e. **Security Technology.** The service shall use Secure Socket Layer ("SSL"), or equivalent technology to protect data from unauthorized access. The service security measures shall include server authentication and data. Provider shall host data pursuant to the Service Agreement in an environment using a firewall that is periodically updated according to industry standards.
- f. **Security Coordinator.** Provider shall provide the name and contact information of Provider's Security Coordinator for the Student Data received pursuant to the Service Agreement.
- g. **Subprocessors Bound.** Provider shall enter into written agreements whereby Subprocessors agree to be bound to the same requirements and duties as set forth in the terms of this Article V. Provider shall periodically conduct or review compliance monitoring and assessments of Subprocessors to determine their compliance with this Article.

2. **Data Breach.** In the event that Student Data is accessed or obtained by an unauthorized individual, Provider shall provide notification to LEA within a reasonable amount of time of the incident. Provider shall follow the following process:

- a. The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described herein under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.
- b. The security breach notification described above in section 2(a) shall include, at a minimum, the following information:
 - i. The name and contact information of the reporting LEA subject to this section.
 - ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
 - iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the

date range within which the breach occurred. The notification shall also include the date of the notice.

- iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.
 - v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
- c. At LEA's discretion, the security breach notification may also include any of the following:
- i. Information about what the agency has done to protect individuals whose information has been breached.
 - ii. Advice on steps that the person whose information has been breached may take to protect himself or herself.
- d. Any agency that is required to issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. Provider shall assist LEA in these efforts.
- e. At the request and with the assistance of the District, Provider shall notify the affected parent, legal guardian or eligible pupil of the unauthorized access, which shall include the information listed in subsections (b) and (c), above.

ARTICLE VI: GENERAL OFFER OF PRIVACY TERMS

Provider may, by signing the attached Form of General Offer of Privacy Terms ("General Offer"), (attached hereto as Exhibit "E"), be bound by the terms of this DPA to any other LEA who signs the Acceptance on said Exhibit. The Form is limited by the terms and conditions described therein.

ARTICLE VII: MISCELLANEOUS

1. **Term.** The Provider shall be bound by this DPA for the duration of the Service Agreement or so long as the Provider maintains any Student Data. Notwithstanding the foregoing, Provider agrees to be bound by the terms and obligations of this DPA for no less than three (3) years.
2. **Termination.** In the event that either party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated.
3. **Effect of Termination Survival.** If the Service Agreement is terminated, the Provider shall destroy all of LEA's data pursuant to Article V, section 1(b).

4. **Priority of Agreements.** This DPA shall govern the treatment of student records in order to comply with the privacy protections, including those found in FERPA and AB 1584. In the event there is conflict between the terms of the DPA and the Service Agreement, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.
5. **Notice.** All notices or other communication required or permitted to be given hereunder must be in writing and given by personal delivery, facsimile or e-mail transmission (if contact information is provided for the specific mode of delivery), or first class mail, postage prepaid, sent to the addresses set forth herein.

Irvine Unified School District
Attn: Michelle Bennett
5050 Barranca Parkway
Irvine, CA 92604

Oxford University Press
Attn: Library Sales Manager
2001 Evans Road
Cary, NC 27513

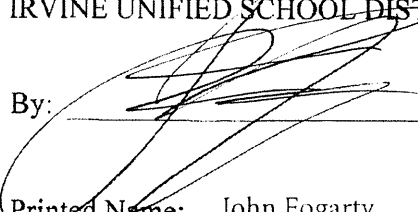
6. **Application of Agreement to Other Agencies.** Provider may agree by signing General Offer of Privacy Terms be bound by the terms of this DPA for the services described therein for any Successor Agency who signs a Joinder to this DPA.
7. **Entire Agreement.** This DPA constitutes the entire agreement of the parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both parties. Neither failure nor delay on the part of any party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.
8. **Severability.** Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.

9. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF CALIFORNIA, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS LOCATED IN ORANGE COUNTY, CALIFORNIA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS SERVICE AGREEMENT OR THE TRANSACTIONS CONTEMPLATED HEREBY.

[Signature Page Follows]

IN WITNESS WHEREOF, the parties have executed this California Student Data Privacy Agreement as of the last day noted below.

IRVINE UNIFIED SCHOOL DISTRICT

By:  _____

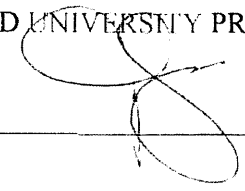
Date: 10/22/2018

Printed Name: John Fogarty

Title/Position: Asst Supt Business Services

USD Board Approved 10/16/2018

OXFORD UNIVERSITY PRESS

By:  _____

Date: 6/15/2018

Printed Name: Jeffrey Shoup

Title/Position: Institutional Sales Manager

Note: Electronic signature not permitted.

EXHIBIT "A"

DESCRIPTION OF SERVICES

Online access to Oxford English Dictionary.

EXHIBIT "B"
SCHEDULE OF DATA

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc	Yes
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	Yes
Assessment	Standardized test scores	
	Observation data	
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications that are captured (emails, blog entries)	Yes
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, preferred or primary language spoken by student)	
	Other demographic information-Please specify:	
Enrollment	Student school enrollment	
	Student grade level	
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
Parent/Guardian Contact Information	Address	
	Email	
	Phone	
Parent/Guardian ID	Parent ID number (created to link parents to students)	
Parent/Guardian Name	First and/or Last	

Category of Data	Elements	Check if used by your system
Schedule	Student scheduled courses	
	Teacher names	
Special Indicator	English language learner information	
	Low income status	
	Medical alerts	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
Category of Data	Other indicator information-Please specify:	
Student Contact Information	Address	
	Email	Yes
	Phone	
Student Identifiers	Local (School district) ID number	
	State ID number	
	Vendor/App assigned student ID number	
	Student app username	
	Student app passwords	
Student Name	First and/or Last	
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	
Student work	Student generated content, writing, pictures etc.	
	Other student work data - Please specify:	

Category of Data	Elements	Check if used by your system
Transcript	Student course grades	
	Student course data	
	Student course grades/performance scores	
	Other transcript data -Please specify:	
Transportation	Student bus assignment	
	Student pick up and/or drop off location	
	Student bus card ID number	
	Other transportation data - Please specify:	
Other	Please list each additional data element used, stored or collected by your application	

EXHIBIT "C"
DEFINITIONS

AB 1584, Buchanan: The statutory designation for what is now California Education Code § 49073.1, relating to pupil records.

De-Identifiable Information (DII): De-Identification refers to the process by which the Vendor removes or obscures any Personally Identifiable Information ("PII") from student records in a way that removes or minimizes the risk of disclosure of the identity of the individual and information about them.

NIST 800-63-3: Draft National Institute of Standards and Technology ("NIST") Special Publication 800-63-3 Digital Authentication Guideline.

Operator: For the purposes of SB 177, SOPIPA, the term "operator" means the operator of an Internet Website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used primarily for K–12 school purposes and was designed and marketed for K–12 school purposes. For the purpose of the Service Agreement, the term "Operator" is replaced by the term "Provider." This term shall encompass the term "Third Party," as it is found in AB 1584.

Personally Identifiable Information (PII): The terms "Personally Identifiable Information" or "PII" shall include, but are not limited to, student data, metadata, and user or pupil-generated content obtained by reason of the use of Provider's software, website, service, or app, including mobile apps, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians. PII includes, without limitation, at least the following:

First and Last Name	Home Address
Telephone Number	Email Address
Discipline Records	Test Results
Special Education Data	Juvenile Dependency Records
Grades	Evaluations
Criminal Records	Medical Records
Health Records	Social Security Number
Biometric Information	Disabilities
Socioeconomic Information	Food Purchases
Political Affiliations	Religious Information
Text Messages	Documents
Student Identifiers	Search Activity
Photos	Voice Recordings
Videos	

General Categories:

Indirect Identifiers: Any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty

Information in the Student's Educational Record

Information in the Student's Email

Provider: For purposes of the Service Agreement, the term "Provider" means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of pupil records. Within the Service Agreement the term "Provider" replaces the term "Third Party as defined in California Education Code § 49073.1 (AB 1584, Buchanan), and replaces the term as "Operator" as defined in SB 177, SOPIPA.

Pupil Generated Content: The term "pupil-generated content" means materials or content created by a pupil during and for the purpose of education including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of pupil content.

Pupil Records: Means both of the following: (1) Any information that directly relates to a pupil that is maintained by LEA and (2) any information acquired directly from the pupil through the use of instructional software or applications assigned to the pupil by a teacher or other local educational LEA employee.

SB 1177, SOPIPA: Once passed, the requirements of SB 1177, SOPIPA were added to Chapter 22.2 (commencing with Section 22584) to Division 8 of the Business and Professions Code relating to privacy.

Service Agreement: Refers to the Contract or Purchase Order to which this DPA supplements and modifies.

School Official: For the purposes of this Agreement and pursuant to CFR 99.31 (B), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of education records; and (3) Is subject to CFR 99.33(a) governing the use and re-disclosure of personally identifiable information from student records.

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, home address, telephone number, email address, or other information allowing online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information text messages, documents, student identifies, search activity, photos, voice recordings or geolocation information. Student Data shall constitute Pupil Records for the purposes of this Agreement, and for the purposes of California and Federal laws and regulations. Student Data as specified in Exhibit B is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or de-identified.

Subscribing LEA: An LEA that was not party to the original Services Agreement and who accepts the Provider's General Offer of Privacy Terms.

Subprocessor: For the purposes of this Agreement, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its software, and

who has access to PII. This term shall also include in it meaning the term "Service Provider," as it is found in SOPIPA.

Targeted Advertising: Targeted advertising means presenting an advertisement to a student where the selection of the advertisement is based on student information, student records or student generated content or inferred over time from the usage of the Provider's website, online service or mobile application by such student or the retention of such student's online activities or requests over time.

Third Party: The term "Third Party" as appears in California Education Code § 49073.1 (AB 1584, Buchanan) means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of pupil records. However, for the purpose of this Agreement, the term "Third Party" when used to indicator the provider of digital educational software or services is replaced by the term "Provider."

EXHIBIT "D"

DATA SECURITY REQUIREMENTS

N/A

EXHIBIT "E"
GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

Provider offer the same privacy protections found in this DPA between it and Irvine Unified School District and which is dated October 17, 2018 to any other LEA ("Subscribing LEA") who accepts this General Offer though its signature below. This General Offer shall extend only to privacy protections and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the other LEA may also agree to change the data provide by LEA to the Provider to suit the unique needs of the LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statues; (2) a material change in the services and products subject listed in the Originating Service Agreement; or three (3) years after the date of Provider's signature to this Form. Provider shall notify the California Student Data Privacy Alliance in the event of any withdrawal so that this information may be transmitted to the Alliance's users.

OXFORD UNIVERSITY PRESS

BY: _____

Date: 6/15/2018

Printed Name: Jeffrey Shoup

Title/Position: Institutional Sales Manager

2. Subscribing LEA

A Subscribing LEA, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA.

BY: _____

Date: _____

Printed Name: _____

Title/Positon: _____

We use cookies to enhance your experience on our website. By clicking 'continue' or by continuing to use our website, you are agreeing to our use of cookies. You can change your cookie settings at any time.

[Find Out More](#) CONTINUE

[Home](#) >

Legal notice

This legal notice is specific to this website ("Website") and overrides any other legal notices appearing elsewhere on Oxford University Press websites. By using the Website, you are agreeing to the practices set out in this statement.

You may access certain parts of the Website without registering or providing OUP with your details.

As the information on the Website may be incomplete, out of date or inaccurate and may contain technical inaccuracies or typographical errors, Oxford University Press ("OUP", "we", "us" or "our") reserve the right to update the Website at our sole discretion. Thus, such information may be changed or updated without notice.

We reserve the right to make changes to this legal notice. Any changes we may make to this legal notice will be posted on this page and, where appropriate, we will also notify you by e-mail. Certain provisions of this legal notice may be superseded by expressly designated legal notices or terms located on particular pages of the Website.

Username and Passwords

Where you have registered on the Website and have been provided with a username and password, you agree not to make available your username and/or password to anyone. If there has been a disclosure of your username and/or password, you agree to notify us promptly of such disclosure so that OUP can take appropriate security measures and to provide you with a new username and password.

Subscribers

Under the licence to access restricted content on the Website accepted by a subscriber (which may be you as an individual or an institution to which you are affiliated) you are permitted to:

1. search, view, retrieve, and display portions of restricted content
2. electronically save portions of restricted content; and/or
3. print out single copies of portions of restricted content

in each case, subject to any specific restrictions which appear on particular pages of the Website. Under the licence accepted by the subscriber, you may not:

1. remove or alter the copyright notices or other means of identification or disclaimers as they appear on the Website;
2. systematically make printed or electronic copies of multiple extracts of restricted content for any purpose except as permitted by law or as authorised by OUP;
3. display or distribute any restricted content on any electronic network, including without limitation on the Internet and the World Wide Web (other than the institution's secure network, where the subscriber is an institution);
4. permit anyone to access or use restricted content (other than other users authorised by the institution, where the subscriber is an institution); and/or
5. use any content on the Website whether restricted content or otherwise for any commercial use.

If you sign up to receive newsletters or subscribe to our web feed you may only use the material sent to you for non-commercial use. You may not:

1. remove or alter the copyright notices or other means of identification or disclaimers as they appear in the material sent to you;
2. systematically make printed or electronic copies of multiple extracts of the material for any purpose except as permitted by law or as authorised by OUP;
3. display or distribute any part of the material on any electronic network, including without limitation the Internet and the World Wide Web;

4. permit anyone to access or use the material, and/or
5. use all or any part of the material for any commercial use.

ClickandBuy customers

If you have purchased a subscription for the Website through ClickandBuy, your subscription contract will be with ClickandBuy and NOT with Oxford University Press, however, your use of the Website will still be subject to the [privacy policy](#) and this legal notice.

Your card will be automatically charged each month until you cancel your subscription.

Intellectual Property Rights

We and/or our licensors are the owners of all intellectual property rights in the Website, and the Website and the materials on the Website are protected by intellectual property laws around the world including copyright and trade mark laws. Subject to the terms of this legal notice and any other licence agreements between you and OUP, all such rights are reserved and no materials may otherwise be copied, modified, published, broadcast or otherwise distributed without our prior written permission. OUP, Oxford and/or any other names of products or services provided by Oxford University Press and referred to on the Website are either trademarks or registered trademarks of Oxford University Press.

Notwithstanding the foregoing and where applicable, copyright in each illustration that appears on the Website is owned by the rights holder(s) named in 'Picture Details' window for that illustration. All rights are reserved. No illustration from the Website may be copied, modified, published or broadcast or otherwise distributed.

Disclaimer

Oxford University Press makes no warranties or representations of any kind concerning the accuracy or suitability of the information contained on the Website for any purpose. All such information is provided "as is" and with a specific disclaimer of any warranties of merchantability, fitness for purpose, title and/or non-infringement. Oxford University Press makes no warranties or representations of any kind that the services provided by this Website will be uninterrupted, error-free or that the Website or the server that hosts the Website are free from viruses or other forms of harmful computer code.

You are solely responsible for your choice in selecting this Website product.

In no event shall Oxford University Press, its employees or agents be liable for any direct, indirect or consequential damages, loss of opportunity, loss of data, loss of goodwill, loss of anticipated savings or loss of profits resulting from the use of the Website even if OUP has been advised of such loss.

Without prejudice to the foregoing paragraph, OUP's liability arising out of or in connection with your use of the Website and/or this legal notice whether in contract, tort, misrepresentation, under statute or otherwise will not exceed the price you paid for your subscription to access this Website.

Neither party's liability for personal injury or death caused by negligence or for fraud is excluded or limited.

The exclusion and limitation set out in this legal notice only applies to the extent permitted by law and is without prejudice to any express provisions to the contrary in any written licence or subscription agreement which you have with Oxford University Press in respect of the use of any online service provided via the Website.

Links

Links to other websites are provided by OUP in good faith and for information only. OUP disclaims any responsibility for the materials contained in any website linked to the Website. In addition, a link to a non-OUP website does not mean that OUP endorses or accepts any responsibility for the content, or the use, of such website or the products and/or services offered on such website. It is up to you to take precautions to ensure that whatever you select for your use is free of such items as viruses, worms, trojans and other items of a destructive nature.

Service Access

While we endeavour to ensure that the Website is normally available 24 hours a day, we shall not be liable if for any reason the Website is unavailable at any time or for any period.

Access to the Website may be suspended temporarily and without notice in the case of system failure, maintenance or repair or for reasons beyond our control.

You are prohibited from posting or transmitting to or from the Website any material

that is threatening, defamatory, obscene, indecent, seditious, offensive, pornographic, abusive, liable to incite racial hatred, discriminatory, menacing, scandalous, inflammatory, blasphemous, in breach of confidence, in breach of privacy or which may cause annoyance or inconvenience,

for which you have not obtained all necessary licences and/or approvals;

which constitutes or encourages conduct that would be considered a criminal offence, give rise to civil liability, or otherwise be contrary to the law of or infringe the rights of any third party, in any

country in the world, or

which is technically harmful (including, without limitation, computer viruses, logic bombs, Trojan horses, worms, harmful components, corrupted data or other malicious software or harmful data).

You may not misuse the Website (including, without limitation, by hacking).

Copyright Infringement Complaints

OUP respects, and takes the protection of intellectual property rights seriously. If you believe that any content on this website infringes your copyright and you wish it to be taken down, please send us a written notice by email or post which includes:

- (i) a physical or electronic signature of the copyright owner or someone authorized to act on behalf of the copyright owner.
- (ii) Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single website are covered by a single notification, a list of such works at that website.
- (iii) Identification of the material that is claimed to be infringing (or to be the subject of infringing activity) which is sufficient to allow OUP to identify and locate the material.
- (iv) Your address, telephone number, and, if available, an email address at which you may be contacted.
- (v) A statement that you have a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.
- (vi) A statement that the information in the notification is accurate, and under penalty of perjury, that you are authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

Please send this notice to our designated DMCA agent:

By email: dmca@oup.com

By post: Legal Department

Oxford University Press

Great Clarendon Street

Oxford

OX2 6DP

United Kingdom

Global Nature of Websites

You recognise the global nature of the Website and thus, agree to comply with all applicable local laws in your jurisdiction when using the Website.

Information we publish on the Website may contain references or cross-references to our services and/or products offered that are not announced or available in your country. Such references do not imply that we intend to announce such services and/or products in your country.

Governing Law

You agree that this legal notice shall be exclusively governed in accordance with the laws of and the courts in England and Wales. Notwithstanding the foregoing, nothing in this legal notice will preclude OUP from applying to any court to bring an action for the infringement of its intellectual property rights.

Queries

If you have any concerns about material which appears on the Website, please contact oxfordonline@oup.com if you are in the Americas or onlinesubscriptions@oup.com if you are outside the Americas.

Note on proprietary status

OED Online include some words which have or are asserted to have proprietary status as trade marks or otherwise. Their inclusion does not imply that they have acquired for legal purposes a non-proprietary or general significance nor any other judgement concerning their legal status. In cases where the editorial staff have some evidence that a word has proprietary status this is indicated in the entry for that word but no judgement concerning the legal status of such words is made or implied thereby.

Thank you for visiting the Website.

OXFORD
UNIVERSITY PRESS

[Cookie policy](#) [About](#) [Privacy policy](#) [Legal notice](#) [@oed](#)

Sign up for OED Word of the Day

[Click here to see our Privacy Policy](#)

Enter e-mail address

